Docket No. 245395US90/hyc

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takehiro NAKAYAMA, et al. GAU:

SERIAL NO: 10/705,818 EXAMINER:

FILED: November 13, 2003

FOR: COMMUNICATION TERMINAL, VALUE ENTITY PROVIDING SERVER, APPLICATION DELIVERY SERVER, ELECTRONIC PROCUREMENT SUPPORTING METHOD, AND ELECTRONIC PROCUREMENT SUPPORTING PROGRAM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2002-338558	November 21, 2002

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

☐ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Bradley D. Lytle
Registration No. 40,073

Joseph A. Scafetta, Jr.
Registration No. 26,803

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

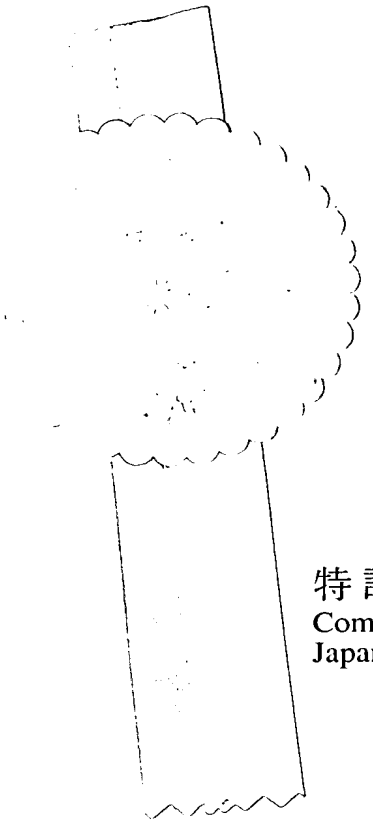
10/705,818

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００２年１１月２１日
出願番号 Application Number:	特願２００２－３３８５５８
[ST. 10/C]:	[ＪＰ２００２－３３８５５８]
出願人 Applicant(s):	株式会社エヌ・ティ・ティ・ドコモ



２００３年１１月１９日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０９５７１１

【書類名】　特許願
【整理番号】　14-0409
【提出日】　平成14年11月21日
【あて先】　特許庁長官殿
【国際特許分類】　H04M 15/00
【発明者】
　【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
　【氏名】　中山　雄大
【発明者】
　【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
　【氏名】　中野　博隆
【特許出願人】
　【識別番号】　392026693
　【氏名又は名称】　株式会社エヌ・ティ・ティ・ドコモ
【代理人】
　【識別番号】　100088155
　【弁理士】
　【氏名又は名称】　長谷川　芳樹
【選任した代理人】
　【識別番号】　100092657
　【弁理士】
　【氏名又は名称】　寺崎　史朗
【選任した代理人】
　【識別番号】　100114270
　【弁理士】
　【氏名又は名称】　黒川　朋也

【選任した代理人】

【識別番号】　100108213

【弁理士】

【氏名又は名称】　阿部　豊隆

【選任した代理人】

【識別番号】　100113549

【弁理士】

【氏名又は名称】　鈴木　守

【手数料の表示】

【予納台帳番号】　014708

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信端末、価値実体提供サーバ、アプリケーション配信サーバ、電子購買支援システム、電子購買支援方法、及び電子購買支援プログラム

【特許請求の範囲】

【請求項１】

特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得手段と、

前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信手段と、

前記公開鍵を使用して前記アプリケーションを検証する検証手段と、

前記検証手段による前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転手段と

を備えることを特徴とする通信端末。

【請求項２】

前記検証手段は、前記受信手段により前記アプリケーションが受信されたことを契機として前記アプリケーションの検証を開始し、

前記検証手段による前記アプリケーションの検証が成功したことを契機として前記アプリケーションを起動する起動手段

を更に備えることを特徴とする請求項１に記載の通信端末。

【請求項３】

前記受信手段により前記アプリケーションが受信された時点から所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段

を更に備えることを特徴とする請求項１又は２に記載の通信端末。

【請求項４】

前記受信手段により前記アプリケーションが受信された後に、当該アプリケーションの送信元との通信が切断された場合に、通信切断時から所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段

を更に備えることを特徴とする請求項１又は２に記載の通信端末。

【請求項５】

請求項１に記載の通信端末に対して、セルラーネットワークを経由して、特定

の秘密鍵に対応する公開鍵が添付された価値実体を提供する提供手段を備えることを特徴とする価値実体提供サーバ。

【請求項６】

前記提供手段は、価値実体の提供に先立って、当該価値実体とは別に前記公開鍵を前記通信端末に送信することを特徴とする請求項５に記載の価値実体提供サーバ。

【請求項７】

前記公開鍵は、セルラーネットワークを経由して複数の端末からアクセス可能なサーバ上に公開されていることを特徴とする請求項５に記載の価値実体提供サーバ。

【請求項８】

前記提供手段により前記価値実体が提供される前に、前記通信端末のインテグリティを検証する第２検証手段を更に備えることを特徴とする請求項５に記載の価値実体提供サーバ。

【請求項９】

請求項１に記載の通信端末に対して、アドホックネットワークを経由して、前記アプリケーションを送信するアプリケーション送信手段と、

前記通信端末の移転手段により移転された価値実体を、前記アドホックネットワークを経由して取得する価値実体取得手段と

を備えることを特徴とするアプリケーション配信サーバ。

【請求項１０】

前記価値実体取得手段により前記価値実体が取得された場合に、当該価値実体が受領された旨が電子的に表現された領収書データを、前記アドホックネットワークを経由して前記通信端末に送信する領収書送信手段

を更に備えることを特徴とする請求項９に記載のアプリケーション配信サーバ。

【請求項１１】

前記送信手段により前記アプリケーションが送信される前に、前記通信端末のインテグリティを検証する第３検証手段を更に備えることを特徴とする請求項９に記載のアプリケーション配信サーバ。

【請求項１２】

請求項１に記載の通信端末と、請求項５に記載の価値実体提供サーバと、請求項９に記載のアプリケーション配信サーバとを備えて構成され、

前記通信端末は、前記価値実体提供サーバから提供された価値実体を取得すると共に、前記アプリケーション配信サーバから受信されたアプリケーションを使用して前記価値実体を移転することを特徴とする電子購買支援システム。

【請求項１３】

通信端末が、取得手段により、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得ステップと、

前記通信端末が、受信手段により、前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信ステップと、

前記通信端末が、検証手段により、前記公開鍵を使用して前記アプリケーションを検証する検証ステップと、

前記通信端末が、前記検証手段による前記アプリケーションの検証が成功した場合に、移転手段により、当該アプリケーションを使用して前記価値実体を移転する移転ステップと

を含むことを特徴とする電子購買支援方法。

【請求項１４】

通信端末により実行可能な電子購買支援プログラムにおいて、

特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得機能と、

前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信機能と、

前記公開鍵を使用して前記アプリケーションを検証する検証機能と、

前記検証機能による、前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転機能と

を前記通信端末に実現させることを特徴とする電子購買支援プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信端末、価値実体提供サーバ、アプリケーション配信サーバ、電子購買支援システム、電子購買支援方法、及び電子購買支援プログラムに関する。

【０００２】

【従来の技術】

近年、携帯電話などの携帯型通信端末（以下、「携帯端末」と記す。）の普及や無線通信速度の高速化に伴い、インターネット等のネットワークを介して、携帯端末がサーバ装置から所望のコンテンツデータを取得することが可能な情報通信システムが実用化されている。この様なシステムを利用した電子商取引においては、クレジットカードや現金を使用しない代金支払い手段として、価値実体が使用されることがある。

【０００３】

価値実体とは、電子化されたデータで何らかの経済価値が表現（化体）されたものである。価値実体は、電子バリューと称されることもあり、例えば、貨幣価値が表現された電子マネー（電子貨幣或いは電子通貨などと称されることもある。）の他に、プリペイド方式で提供される電子チケット等がある。電子チケットには、例えば、図書券、回数券、乗車券などの価値が表現されている。

【０００４】

かかる価値実体を安全に流通する方法としては、例えば、耐タンパー性を有するＩＣ（Integrated Circuit）カードに充填（チャージ）された価値実体を、専用のカードリーダを用いて移転させる技術が提案されている（例えば、非特許文献１参照。）。

【０００５】

しかし、ＩＣカードは、携帯性や可搬性に優れている反面、例えば、以下に示す様な問題点もある。

１．ユーザインタフェースをもたないので、別体の表示装置に接続しなければ、価値実体の残量を確認できない。

２．アプリケーションを実装できないので、ユーザに対して、電子購買活動をグラフィカルにナビゲートできない。

３．通信手段をもたないので、別体の通信装置に接続しなければ、価値実体を充填できない。

【０００６】

一方で、携帯性に優れ、かつ、上記問題点を有さない携帯端末として、携帯電話がある。携帯電話は、表示装置などのユーザインタフェースを有すると共に、アプリケーションを実装可能である。また、無線通信手段により、外部のサーバ装置から価値実体を充填することもできる。

【０００７】

携帯電話がアプリケーションを取得する際には、セルラーネットワーク経由でダウンロードするのが一般的である。セルラーネットワークとは、通信事業者が運営する無線基地局などのインフラストラクチャを利用した無線公衆網である。しかし、アプリケーションの中には、安全性が保証されていないものもあり、ダウンロードして実行した際に、携帯電話に危害が及ぶ場合がある。

【０００８】

かかる懸念を解消するために、セルラーネットワークでは、携帯電話内の特定のメモリ領域に対するアプリケーションのアクセスを制限すると共に、アプリケーションを使用して通信できるサーバをその配信元に限定する、といった手法が採られている（例えば、非特許文献２参照。）。

【０００９】

また、他のセルラーネットワークには、正規の作成元として認定された者により作成されたアプリケーションだけがＷｅｂサイトからダウンロードできる仕様になっているものもある（例えば、非特許文献３参照。）。

【００１０】

【非特許文献１】

「電子マネーを構成する情報セキュリティ技術と安全性評価」IMES Discussion Paper Series 98-J-26、 1998年11月、日本銀行金融研究所

【非特許文献２】

ｉモード対応　Ｊａｖａコンテンツ開発ガイド　詳細編　第１．１版、平成13年5月14日、株式会社ＮＴＴドコモ、http://www.nttdocomo.co.jp/p_s/

imode/java/pdf/jguide010514.pdf

【非特許文献３】

Ｊ－ＰＨＯＮＥ　Ｊａｖａアプリ開発ガイド Version 1.1.5, Nov.28, 2001、http://www.dp.j-phone.com/file/j_java_dg115.pdf

【００１１】

【発明が解決しようとする課題】

このように、上記従来技術では、セルラーネットワークにおける価値実体の流通の安全性を確保すべく、人手を掛けて安全性を検証したアプリケーションのみを流通させたり、携帯端末の通信相手を制限したりしている。しかしながら、これらの手法は、セルラーネットワークの利用を前提とするものであり、アドホックネットワークを経由して取得されたアプリケーションの使用を想定したものではなかった。

【００１２】

セルラーネットワークは、通信事業者の管理下にある、言わば閉じたネットワークであり、通信相手の認証が正確に行われる可能性が高い。このため、セルラーネットワークを利用する通信では、第三者が介入する恐れが低く、比較的安全である。これに対して、アドホックネットワークは、無線基地局などの特定のインフラストラクチャに依存せず携帯端末間で一時的に形成される、言わばオープンなネットワークである。したがって、アドホックネットワークから取得されたアプリケーションが、携帯端末に充填された価値実体にアクセスすることには危険の伴う可能性がある。

【００１３】

そこで、上記問題点に鑑みて、本発明は、アドホックネットワークを経由して取得されたアプリケーションを使用して、安全かつ容易に価値実体の授受を行うことを課題とする。

【００１４】

【課題を解決するための手段】

上記課題を解決するために、本発明に係る通信端末は、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得手段と、前記秘密鍵によって電子

署名されたアプリケーションをアドホックネットワークを経由して受信する受信手段と、前記公開鍵を使用して前記アプリケーションを検証する検証手段と、前記検証手段による前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転手段とを備える。

【００１５】

本発明に係る価値実体提供サーバは、上述した通信端末に対して、セルラーネットワークを経由して、特定の秘密鍵に対応する公開鍵が添付された価値実体を提供する提供手段を備える。

【００１６】

本発明に係るアプリケーション配信サーバは、上述した通信端末に対して、アドホックネットワークを経由して、前記アプリケーションを送信するアプリケーション送信手段と、前記通信端末の移転手段により移転された価値実体を、前記アドホックネットワークを経由して取得する価値実体取得手段とを備える。

【００１７】

本発明に係る電子購買支援システムは、上述した通信端末と、上述した価値実体提供サーバと、上述したアプリケーション配信サーバとを備えて構成される。前記通信端末は、前記価値実体提供サーバから提供された価値実体を取得すると共に、前記アプリケーション配信サーバから受信されたアプリケーションを使用して前記価値実体を移転することを特徴とする電子購買支援システムを構築してもよい。

【００１８】

本発明に係る電子購買支援方法は、通信端末が、取得手段により、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得ステップと、前記通信端末が、受信手段により、前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信ステップと、前記通信端末が、検証手段により、前記公開鍵を使用して前記アプリケーションを検証する検証ステップと、前記通信端末が、前記検証手段による前記アプリケーションの検証が成功した場合に、移転手段により、当該アプリケーションを使用して前記価値実体を移転する移転ステップとを含む。

【００１９】

本発明に係る電子購買支援プログラムは、通信端末により実行可能な電子購買支援プログラムにおいて、特定の秘密鍵に対応する公開鍵が添付された価値実体を取得する取得機能と、前記秘密鍵によって電子署名されたアプリケーションをアドホックネットワークを経由して受信する受信機能と、前記公開鍵を使用して前記アプリケーションを検証する検証機能と、前記検証機能による、前記アプリケーションの検証が成功した場合に、当該アプリケーションを使用して前記価値実体を移転する移転機能とを前記通信端末に実現させる。

【００２０】

これらの発明によれば、特定の秘密鍵に対応する公開鍵が添付された価値実体が価値実体提供サーバから通信端末に提供されると共に、前記秘密鍵によって電子署名されたアプリケーションがアドホックネットワークを経由してアプリケーション配信サーバから通信端末宛に送信される。前記アプリケーションは、前記公開鍵を使用して検証される。検証が成功した場合には、当該アプリケーションを使用して、前記価値実体の少なくとも一部が対価としてアプリケーション配信サーバに移転される。これにより、価値実体の提供元とアプリケーションへの署名元との同一性を確認した上で、価値実体に対するアプリケーションへのアクセスを許可することできる。したがって、通信事業者が介在しないアドホックネットワークを経由して取得されたアプリケーションを使用しても、安全かつ容易に価値実体の授受を行うことが可能となる。

【００２１】

本発明に係る通信端末において、前記検証手段は、前記受信手段により前記アプリケーションが受信されたことを契機として前記アプリケーションの検証を開始し、前記検証手段による前記アプリケーションの検証が成功したことを契機として前記アプリケーションを起動する起動手段を更に備えるものとしてもよい。

【００２２】

本発明によれば、アプリケーションは、受信されたことを契機として検証され、検証が成功したことを契機として起動される。これにより、受信されたアプリケーションが正規のものである場合には、通信端末のユーザからの指示を待たず

に、安全なアプリケーションが起動される。したがって、通信端末のユーザは、取得したアプリケーションを簡易迅速に使用することができる。

【００２３】

本発明に係る通信端末において、前記受信手段により前記アプリケーションが受信された時点から所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段を更に備えるものとしもよい。

【００２４】

本発明によれば、アプリケーションは、受信された時点から所定時間が経過したことを契機として削除される。これにより、通信端末のユーザからの指示を待たずに、アプリケーションが削除される。したがって、通信端末のユーザが、かかるアプリケーションを、該アプリケーションに適当でない電子商取引（例えばサービス内容の異なる電子商取引）に誤って使用すること等により、電子商取引に混乱が生じることがない。その結果、電子購買支援の信頼性が維持される。

【００２５】

本発明に係る通信端末において、前記受信手段により前記アプリケーションが受信された後に、当該アプリケーションの送信元との通信が切断された場合に、所定時間が経過したことを契機として、前記アプリケーションを削除する削除手段を更に備えるものとしもよい。

【００２６】

本発明によれば、アプリケーションは、通信端末と送信元との通信が切断された場合に、通信切断時から所定時間が経過したことを契機として削除される。すなわち、通信端末のユーザからの指示を待たずに、アプリケーションの送信元（例えば、アプリケーション配信サーバ）と通信端末との通信が切断された時点から所定時間経過後にアプリケーションは削除される。これにより、アプリケーションが使用される環境から通信端末のユーザが離れたことに伴って、該アプリケーションが削除されることになり、適当でない電子商取引にアプリケーションが使用されることを確実に防止できる。したがって、電子商取引に混乱が生じることがない。その結果、電子購買支援の信頼性が維持される。

【００２７】

本発明に係る価値実体提供サーバにおいて、前記提供手段は、価値実体の提供に先立って、当該価値実体とは別に前記公開鍵を前記通信端末に送信するものとしもよい。

本発明によれば、価値実体は、公開鍵の送信とは別に価値実体提供サーバから通信端末に提供される。したがって、価値実体提供サーバが価値実体を通信端末に補充する際に、価値実体に公開鍵を添付する必要がないので、価値実体提供サーバと通信端末との間における通信負荷の低減を図ることができる。

【００２８】

本発明に係る価値実体提供サーバにおいて、前記公開鍵は、セルラーネットワークを経由して複数の端末からアクセス可能なサーバ上に公開されているものとしもよい。

本発明によれば、公開鍵は、価値実体とは独立して、サーバ（例えば価値実体提供サーバ）上に公開されている。これにより、通信端末は、価値実体を使用する際にのみ、サーバにアクセスして公開鍵を取得することが可能となる。したがって、通信端末は、常に公開鍵を保持する必要がなくなり、記憶容量を節約できる。

【００２９】

本発明に係る価値実体提供サーバにおいて、前記提供手段により前記価値実体が提供される前に、前記通信端末のインテグリティを検証する第２検証手段を更に備えるものとしもよい。本発明によれば、価値実体提供サーバから通信端末に価値実体が提供される前に、通信端末が想定された通りに正常に動作するか否かを示す指標であるインテグリティ（言わば通信端末の信頼性）が検証される。したがって、信頼性の低い通信端末が価値実体を取得することに起因して生じ得る、通信端末のユーザや価値実体の提供元の危害が回避される。

【００３０】

本発明に係るアプリケーション配信サーバは、前記価値実体取得手段により前記価値実体が取得された場合に、当該価値実体が受領された旨が電子的に表現された領収書データを、前記アドホックネットワークを経由して前記通信端末に送信する領収書送信手段を更に備えるものとしもよい。

【００３１】

本発明によれば、アプリケーション配信サーバが価値実体を受領した旨が電子的に表現された領収書データが、アドホックネットワークを経由して、アプリケーション配信サーバから通信端末に送信される。したがって、通信端末が受信した領収書データをユーザが提示することで、アプリケーション配信サーバは、価値実体の送信元が上記通信端末であることを容易に確認することができる。これにより、異なる通信端末（価値実体を送信していない通信端末）のユーザに対して、価値実体の対価としての商品や役務が誤って提供されることをより確実に防止することが可能となる。

【００３２】

本発明に係るアプリケーション配信サーバは、前記送信手段により前記アプリケーションが送信される前に、前記通信端末のインテグリティを検証する第３検証手段を更に備えるものとしもよい。本発明によれば、アプリケーション配信サーバから通信端末にアプリケーションが提供される前に、通信端末が想定された通りに正常に動作するか否かを示す指標であるインテグリティが検証される。したがって、信頼性の低い通信端末がアプリケーションを取得することに起因して、通信端末のユーザやアプリケーションの送信元が危害を被ることが未然に回避される。

【００３３】

【発明の実施の形態】

（第１の実施の形態）

以下、添付図面を参照して本発明の第１の実施の形態に係る電子購買支援システムについて説明する。まず、構成を説明する。図１は、本実施の形態における電子購買支援システム１の全体構成の一例を示す模式図である。図１に示すように、電子購買支援システム１は、価値提供サーバ１０（価値実体提供サーバに対応）と、携帯端末２０（通信端末に対応）と、店舗サーバ３０（アプリケーション配信サーバに対応）とを備えて構成されている。

【００３４】

更に、価値提供サーバ１０と携帯端末２０との間には、セルラーネットワーク

Ｎ１が形成され、携帯端末２０は、基地局Ｂ及びセルラーネットワークＮ１を経由して価値提供サーバ１０との間で、相互に各種データの送受信が可能である。セルラーネットワークＮ１は、通信事業者の管理下にあり、利用者間の通信に際しては、必要に応じて通信相手の認証が行われる。このため、セルラーネットワークＮ１を経由する通信に関しては、第三者が不正に介入する危険性が低く、比較的安全なデータ送受信を実現可能である。

【００３５】

また、携帯端末２０と店舗サーバ３０との間には、アドホックネットワークＮ２が形成され、携帯端末２０は、アドホックネットワークＮ２を経由して店舗サーバ３０との間で、相互に各種データの無線通信が可能である。アドホックネットワークＮ２は、特定のインフラストラクチャに依存せず、携帯端末間で一時的に形成されるネットワークである。本実施の形態では、アドホックネットワークＮ２は、ＩＥＥＥ８０２．１１ｂやＢｌｕｅｔｏｏｔｈ等の近距離無線通信規格に準拠した通信網として説明するが、これに限らず、例えばＩｒＤＡ（Infrared Data Association）、ＩＳＯ１５６９３、ＩＳＯ１４４４３等の近傍無線通信規格に準拠した通信網であってもよい。更には、有線通信網であってもよい。

【００３６】

アドホックネットワークＮ２には、拠点となる端末から送信される電波の到達距離に応じて、通信エリアが限定されるという特性がある。したがって、通信相手の位置を特定することが容易であり、携帯端末のロケーションに適応した電子購買支援用のアプリケーションプログラムを配信するのに適している。また、アドホックネットワークＮ２は、セルラーネットワークＮ１と比較して高速かつ安価な通信を実現できるので、アプリケーションの様な容量の大きなデータの配信に適している。反面、通信事業者の管理下にないので、悪意や瑕疵のあるアプリケーションが流通する可能性も否定できない。

【００３７】

価値提供サーバ１０は、ペイメントサービスプロバイダにより運用され、電子購買（電子的に表現された価値実体を用いて商品や役務を売買すること）に際して使用可能な価値実体の発行及び管理（有償無償提供を含む）を行うサーバ装置

である。価値提供サーバ１０は、セルラーネットワークＮ１を経由して、携帯端末２０に価値実体を提供する。なお、価値提供サーバ１０は、インターネット等の外部ネットワーク上に存在してもよい。この場合、携帯端末２０は、通信事業者が運営するゲートウェイを介して、セルラーネットワークＮ１経由で価値提供サーバ１０にアクセスできる。この際、通信安全性を確保する観点から、ＳＳＬ（Secure Socket Layer）等の所定のセキュアプロトコルを利用して暗号通信を行ってもよい。

【００３８】

携帯端末２０は、複数の通信チャネルに対応しており、本実施の形態では、少なくともセルラーネットワークＮ１及びアドホックネットワークＮ２を経由した通信が可能である。携帯端末２０は、価値提供サーバ１０から価値実体を取得する。携帯端末２０は、店舗サーバ３０から電子購買用のアプリケーションを取得すると共に、該アプリケーションを使用して、上記価値実体を対価とした所望の商品又は役務の購入を支援する。また、携帯端末２０は、耐タンパー性を有するデータ格納領域（メモリ）及び暗号演算処理能力を備える。

【００３９】

店舗サーバ３０は、電子購買が実際に行われる店舗により運用され、電子購買用のアプリケーションを携帯端末２０に提供する。店舗サーバ３０は、電子購買の利用に供される価値実体を商品又は役務の対価として携帯端末２０から取得する。

【００４０】

図２は、本実施の形態における電子購買支援システム１の機能的構成を示すシステム構成図である。図２に示すように、価値提供サーバ１０は、機能的には、価値実体格納部１１と価値実体送信部１２（提供手段に対応）とを有する。価値実体格納部１１には、アプリケーションの検証に使用される公開鍵Ａ１が添付された価値実体１１ａが格納されている。価値実体送信部１２は、携帯端末２０からの要求に応じて、公開鍵Ａ１が添付された価値実体１１ａを価値実体格納部１１から読み出し、セルラーネットワークＮ１及び基地局Ｂを介して、携帯端末２０宛に該価値実体を送信する。

【００４１】

図２に示すように、携帯端末２０は、機能的には、価値実体受信部２１（取得手段に対応）と、価値実体格納部２２と、アプリケーション受信部２３（受信手段に対応）と、アプリケーション検証部２４（検証手段に対応）と、アプリケーション起動部２５（起動手段に対応）と、アプリケーション削除部２６（削除手段に対応）と、価値実体送信部２７（移転手段に対応）と、領収書受信部２８とを有する。

【００４２】

価値実体受信部２１は、価値提供サーバ１０から送信された価値実体１１ａを受信し、公開鍵Ａ１と共に、価値実体格納部２２に格納する。

価値実体格納部２２には、価値実体受信部２１により受信された価値実体１１ａが格納される。価値実体格納部２２は、価値実体の秘匿性やシステムの信頼性を確保する観点から、耐タンパー性を有することが好適である。耐タンパー性を実現する手段に関しては、周知慣用の技術であるので詳細な説明は省略するが、特別な材質によりデバイスを構成する、ダミー配線を適宜織り交ぜるといった方法が考えられる（記述の非特許文献１参照）。価値実体格納部２２は、例えば、ＵＩＭ（User Identity Module）やＳＩＭ（Subscriber Identity Module）などにより構成される。

アプリケーション受信部２３は、店舗サーバ３０から送信され、電子署名が施されたアプリケーションを受信する。

【００４３】

アプリケーション検証部２４は、悪意や瑕疵のあるアプリケーションにより価値実体が不正に使用されることを防ぐために、アプリケーション受信部２３により受信されたアプリケーションが正当性を保証されたものであるか否かの検証を行う。検証は、受信されたアプリケーションに施された電子署名が、価値実体格納部２２内の価値実体１１ａに添付されている公開鍵Ａ１に対応しているか否かに基づいて行われる。具体的には、電子署名は秘密鍵Ａ２により暗号化されているので、電子署名されたアプリケーションは秘密鍵Ａ２に対応する公開鍵Ａ１によってしか復号できない。したがって、公開鍵Ａ１が秘密鍵Ａ２に対応するもの

でない場合には、携帯端末２０は、上記アプリケーションを実行することはできないことなる。

【００４４】

更に、アプリケーション検証部２４は、正当性を保証されたものと判定された（検証に成功した）アプリケーションに対するアクセスを許可すると共に、正当性を保証されていないものと判定された（検証に失敗した）アプリケーションに対するアクセスを拒否する。

【００４５】

アプリケーション起動部２５は、アプリケーション検証部２４による検証の結果、検証に成功したアプリケーションを起動する。

アプリケーション削除部２６は、アプリケーション検証部２４による検証の結果、検証に失敗したアプリケーションを削除する。

【００４６】

価値実体送信部２７は、アプリケーションの検証に成功し、かつ、携帯端末２０のユーザにより商品又は役務の購入が指示された場合に、その対価に相当する額の価値実体を店舗サーバ３０に送信する。

領収書受信部２８は、店舗サーバ３０から送信される、価値実体を受領した旨を示す領収書データを受信する。

【００４７】

図２に示すように、店舗サーバ３０は、機能的には、アプリケーション格納部３１と、アプリケーション送信部３２（アプリケーション送信手段に対応）と、価値実体受信部３３（価値実体取得手段に対応）と、領収書送信部３４（領収書送信手段に対応）とを有する。

【００４８】

アプリケーション格納部３１には、店舗サーバ３０が設置されている店舗における電子購買を可能とするためのアプリケーション３１ａが格納されている。このアプリケーション３１ａは、その提供元によって予め電子署名が施されており、無償又は有償で提供される。アプリケーション３１ａは、価値提供サーバ１０の運用元であるペイメントサービスプロバイダが所持又は管理する秘密鍵Ａ２に

より電子署名されている。電子署名は、アプリケーションの提供元を証明すると共に、アプリケーションの正当性を保証するものであり、この電子署名が付されることにより、アプリケーション３１ａは、秘密鍵Ａ２に対応する公開鍵Ａ１が添付された価値実体の使用が可能となる。

【００４９】

アプリケーション送信部３２は、携帯端末２０からの要求に応じて、アプリケーション３１ａをアプリケーション格納部３１から読み出し、アドホックネットワークＮ２を経由して、携帯端末２０宛にアプリケーション３１ａを送信する。

価値実体受信部３３は、携帯端末２０の価値実体送信部２７により送信された価値実体をアドホックネットワークＮ２を介して受信する。

領収書送信部３４は、提供された商品又は役務の対価に相当する額の価値実体が受信されたことに伴い、その旨を示す領収書データを携帯端末２０宛に作成及び送信する。

【００５０】

携帯端末２０は、本発明に係る電子購買支援システムの主要部を構成する端末装置であるので、以下、そのハードウェア構成について詳細に説明する。図３は、携帯端末２０のハードウェア構成図である。携帯端末２０は、制御装置２０ａ、入力装置２０ｂ、ＲＡＭ２０ｃ、表示装置２０ｄ、記憶装置２０ｅ、アンテナＡを伸縮可能に有するセルラーネットワーク通信装置２０ｆ、音声処理装置２０ｇ、及びアドホックネットワーク通信装置２０ｈを備えて構成される。これら各装置は、それぞれバス２０ｊによって電気的に接続されており、相互に信号の入出力が可能となっている。

【００５１】

制御装置２０ａは、記憶装置２０ｅに記憶されている電子購買支援プログラムをＲＡＭ２０ｃに読み出し、当該プログラムに従って各部を集中制御する。すなわち、制御装置２０ａは、入力装置２０ｂからの入力信号とＲＡＭ２０ｃに読み出されたプログラムとに従って、後述の電子購買処理を始めとする各種処理を実行し、その処理結果をＲＡＭ２０ｃに一時的に記憶する。そして、ＲＡＭ２０ｃに記憶された処理結果を必要に応じて記憶装置２０ｅ内部の所定領域に格納させ

る。

【００５２】

入力装置２０ｂは、価値実体及びアプリケーションの送信要求、商品又は役務の選択及び購入等を指示する各種操作ボタンを備えて構成され、これら各種操作ボタンは、単独で又は組み合せて押下されることにより、指示内容に応じた入力信号を制御装置２０ａに出力する。

【００５３】

ＲＡＭ（Random Access Memory）２０ｃは、揮発性の半導体メモリにより構成され、制御装置２０ａにより実行される各種処理において、後述する記憶装置２０ｅから読み出されたプログラムやデータを一時的に格納する。また、ＲＡＭ２０ｃは、表示装置２０ｄに表示されるデータを一時的に記憶するＶＲＡＭ（Video RAM）の機能も併有する。

【００５４】

表示装置２０ｄは、ＬＣＤ（Liquid Crystal Display）やＥＬ（Electro Luminescence）等により構成され、制御装置２０ａから入力される表示信号に従って、商品メニュー等の表示データの表示を行うユーザインタフェースである。

【００５５】

記憶装置２０ｅは、ＥＥＰＲＯＭ（Electrically Erasable and Programmable ROM）等の不揮発性の半導体メモリにより構成され、各種処理の実行に際して必要なデータや各種処理の実行の結果生成されたデータ等を記憶する。また、記憶装置２０ｅには、上述した価値実体が格納される。

【００５６】

セルラーネットワーク通信装置２０ｆは、基地局Ｂとの無線通信の制御を行う。詳細には、セルラーネットワーク通信装置２０ｆは、信号の変調及び復調を行う変復調部（図示せず）と、信号の符号化及び復号化を行う符復号化部（図示せず）とを有する回路であり、アンテナＡを有する。アンテナＡは、携帯端末２０の筐体上部に伸縮可能に設けられ、基地局Ｂとの間で電波の送受信を行う。

【００５７】

音声処理装置２０ｇは、変換器、増幅器等により構成され、マイクＭ及びスピ

ーカＳを備える。音声処理装置２０ｇは、通話時に、制御装置２０ａから入力される音声データを変換器でアナログ信号に変換し、増幅器を介してスピーカＳから放音する。また、音声処理装置２０ｇは、通話時に、マイクＭから入力される音声信号を変換器によりデジタル信号に変換し、制御装置２０ａに出力する。

【００５８】

アドホックネットワーク通信装置２０ｈは、無線ＬＡＮの標準規格であるＩＥＥＥ８０２．１１ｂあるいはＢｌｕｅｔｏｏｔｈ等の近距離無線通信規格に準拠しており、アドホックネットワークＮ２との間で直接的にデータの送受信を行う。

【００５９】

次に、本実施の形態における電子購買支援システム１の動作について説明すると共に、併せて、本発明に係る電子購買支援方法を構成する各ステップについて説明する。

【００６０】

本実施の形態では、電子購買処理が実行される店舗として、特に、コーヒーショップのチェーン店を想定するが、本発明は、かかる店舗においてのみ適用されるものではない。本実施形態におけるチェーン店とは、同種の商品又は役務を統一された商号の下で取り扱う店舗であって、同一の本部の管理下で利益を実現する経営組織形態である。また、価値提供サーバ１０の運用主体であるペイメントサービスプロバイダは、商品又は役務の販売に関する契約を上記本部と結んでいる。なお、該本部が、ペイメントサービスプロバイダを兼ねてもよい。

【００６１】

図４は、電子購買支援システム１によって実行される電子購買処理の流れを示すフローチャートである。以下に示す各ステップは、図３に示した記憶装置２０ｅに格納されている電子購買支援プログラムが、制御装置２０ａによって実行されることにより実現する。

【００６２】

まず、携帯端末２０のユーザが、クレジットカードによる電子決済や通信事業者による代行課金などの商取引により価値実体を購入する。これに伴い、価値提

供サーバ１０の価値実体送信部１２により、公開鍵Ａ１が添付された価値実体１１ａが、セルラーネットワークＮ１及び基地局Ｂ経由で携帯端末２０宛に送信される（Ｓ１）。かかる送信処理は、既存の電子商取引の技術により実現可能であるが、第三者によるなりすましを防止するために、予め登録されたパスワードによる認証や認証局による電子認証を利用することが望ましい。

【００６３】

ここで、電子商取引にて提供される多種多様なサービスの中から、価値実体１１ａを対価として所望の商品を購入する電子購買サービスを明確に識別するために、必要に応じて、該サービスを一意に特定可能な識別子（以下、「サービス識別子」と記す。）を価値実体１１ａに付与しておくことが好ましい。サービス識別子は、他のサービスとの重複を回避すべく、例えば、価値提供サーバ１０のＩＰアドレスと、価値提供サーバ１０により生成される文字列の内、過去に使用されていない文字列とが組み合わせられたデータである。

【００６４】

サービス識別子は、価値実体１１ａを使用可能なアプリケーションによっても保持されている。かかる識別子は、例えば、アプリケーションのファイル名を示す文字列に含まれている、あるいは、アプリケーションに明示的に割り当てられたメタ情報記述領域に記述されている。したがって、携帯端末２０は、アプリケーションを実行する前に、当該アプリケーションにより特定されるサービスが、価値実体１１ａを使用するサービスと一致するか否かを検知することができる。

【００６５】

Ｓ２では、Ｓ１で送信された価値実体１１ａが、携帯端末２０の価値実体受信部２１により受信され、サービス識別子と対応付けて、価値実体格納部２２に格納される。

【００６６】

Ｓ３では、携帯端末２０は、アドホックネットワークＮ２を介して店舗サーバ３０に接続される。かかる接続は、例えば、店舗としてのコーヒーショップ内で店舗サーバ３０により形成される無線ＬＡＮの通信エリア内に携帯端末２０が在圏したことに伴い、アドホックネットワーク通信装置２０ｈにより確立される。

通常、無線ＬＡＮの通信エリアは、コーヒーショップの敷地及びその近傍であるので、遅くとも携帯端末２０のユーザが入店した時点で、携帯端末２０と店舗サーバ３０との間でアドホックネットワークを経由した通信が可能な状態になる。

【００６７】

Ｓ４では、店舗サーバ３０のアプリケーション送信部３２により、秘密鍵Ａ２により電子署名されたアプリケーション３１ａが、アドホックネットワークＮ２経由で携帯端末２０宛に送信される。かかる送信処理は、店舗サーバ３０が、携帯端末２０を含む携帯端末に対してアプリケーションを強制的に送信するプッシュ型送信であってもよいし、携帯端末２０からの能動的な送信要求を待って送信するプル型送信であってもよい。

【００６８】

Ｓ４で送信されるアプリケーション３１ａは、チェーン店における購買支援を目的とするものであり、店舗サーバ３０が設置されるコーヒーショップに特化したマーケティング戦略や独自のサービス品目又は商品種別に応じて、その設計内容は個別に選定される。また、アプリケーション３１ａは、適宜更新可能である。これにより、店舗の特性や経時的変化に適応した効果的な購買支援を可能とする。

【００６９】

Ｓ５では、Ｓ４で送信されたアプリケーション３１ａが、携帯端末２０のアプリケーション受信部２３により受信され、アプリケーション検証部２４により、公開鍵Ａ１及び電子署名を使用した正当性の検証が行われる。

【００７０】

ここで、価値実体格納部２２に複数種の価値実体が格納されている場合には、検証処理の高速化を図る観点から、検証対象となる価値実体を極力限定する処理が有効となるが、当該処理は、携帯端末２０が、上述したサービス識別子をアプリケーションのファイル名等から検知することにより実現可能である。以下、図５を参照しながら、複数種の価値実体が格納されている場合に好適なアプリケーション検証処理について説明する。

【００７１】

図５は、相互に異なる公開鍵が添付された複数の価値実体が格納された価値実体格納部２２内のデータ格納例を示す図である。図５に示す様に、価値実体格納部２２は、価値実体領域２２１とサービス識別子領域２２２とを少なくとも備える。価値実体領域２２１には、価値提供サーバ１０から提供された価値実体１１ａの他に、公開鍵Ａ１とは異なる公開鍵Ａ２，Ａ３，Ａ４がそれぞれ添付された価値実体が格納されている。サービス識別子領域２２２には、対応する価値実体領域２２１内の価値実体が使用されるサービスの識別子（例えば、“0001”，“0002”，“0003”，…）が格納されている。

【００７２】

図４に戻り、Ｓ５において、アプリケーション検証部２４は、受信されたアプリケーションにより特定されるサービス識別子と、サービス識別子領域２２２内のサービス識別子とを照合する。照合の結果、アプリケーションのサービス識別子に一致するサービス識別子が検知されなかった場合には、その時点で、当該アプリケーションの検証に失敗したことになり、後述のＳ１３以降の処理に移行する。

【００７３】

一方、上記照合の結果、アプリケーションのサービス識別子に一致するサービス識別子が検知された場合には、アプリケーションが正当性を有する可能性もあるが、同一のサービス識別子を有する複数の価値実体が検知される可能性、あるいは、アプリケーションの電子署名が価値実体の公開鍵に対応していない可能性も依然としてある。

【００７４】

そこで、アプリケーション検証部２４は、更に、サービス識別子が一致した価値実体に添付された公開鍵を用いて、受信されたアプリケーションの電子署名を検証する。すなわち、アプリケーション検証部２４は、上記アプリケーションが、価値実体の提供元であるペイメントサービスプロバイダによって電子署名されたものであるか、及び、改竄されていないかを検証する。かかる検証は、例えば公開鍵暗号方式により実現可能である。なお、アプリケーションの検証処理は、アプリケーションの受信を契機として自動的に実行されるものとしてもよいし、

ユーザによる入力装置２０ｂからの指示を待って実行されるものとしてもよい。

【００７５】

また、価値実体格納部２２内に一の価値実体しか格納されていない場合には、サービス識別子の照合処理を行わず、電子署名の検証処理のみを行うものとしてもよい。

その結果、アプリケーション３１ａのサービス識別子である“０００１”を有し、かつ、秘密鍵Ａ２に対応する公開鍵Ａ１が添付された価値実体、つまり価値実体１１ａの検証は成功する。

【００７６】

Ｓ５における検証の結果、アプリケーションの電子署名が価値実体の提供元によって為され、かつ、アプリケーションが改竄されていないものであることが確認されると、アプリケーション検証部２４は、アプリケーションの検証に成功したものと判断し（Ｓ６；Ｙｅｓ）、アプリケーション起動部２５に対して、アプリケーションの起動を指示する。

【００７７】

Ｓ７では、Ｓ５で受信されたアプリケーションは、アプリケーション起動部２６により起動される。起動されたアプリケーション３１ａは、Ｓ２で受信及び格納された価値実体１１ａに対するアクセスが可能である。アプリケーション３１ａの起動に伴い、携帯端末２０のユーザが購買可能な商品又は役務が掲載されたメニューリストが表示装置２０ｄに表示され、制御装置２０ａは、ユーザによる入力装置２０ｂからの購買指示を待機する。購買指示には、ユーザが購買を希望する商品又は役務の識別情報の指定はもとより、個数の指定をも含む。

【００７８】

例えば、店舗が上述したチェーン店である場合には、図６に示すコーヒーショップメニュー２０１が表示装置２０ｄに表示される。図６に示す様に、コーヒーショップメニュー２０１には、複数のコーヒーの種類が商品名として価格と共に記載されている。ユーザは、所望の商品名（ドライカフェラテ）に対応してその左側に位置するチェックボックス２０１ａに、入力装置２０ｂによりチェックすることにより、購買対象となるコーヒーを選択する。チェックボックス２０１ａ

には、所望するコーヒーの個数を入力するようにしてもよい。また、購買対象の選択後に、商品名と個数とをユーザが確認するためのメッセージを表示装置２０ｄに表示させてもよい。

【００７９】

より具体的には、コーヒーショップメニュー２０１において、コーヒーショップが独自にプロモートしている“ドライカフェラテ”が、ユーザの目に留まり易い位置（メニューの冒頭部分に近い領域）に“当店のお薦め”として表示されている。このようにして、電子購買支援システム１は、上記本部の管理下にあるコーヒーショップ毎に、独自のマーケティング戦略やロケーションに即した電子購買支援を可能とする。特に、全国展開するチェーン店では、ユーザの嗜好や気象条件が地域毎に異なるので、各コーヒーショップ毎に異なる電子購買支援を行うことは、利便性向上や販売促進の観点から効果的である。更に、“本日のコーヒー”に表示される商品名を適宜（例えば毎日）変更することも、ユーザニーズの変化に即応する意味で有効である。

【００８０】

図４に戻り、購買指示が入力されると（Ｓ８）、携帯端末２０の価値実体送信部２７により、購買を指示された商品又は役務の対価に相当する額（上記例では３５０円）の価値実体が、価値実体格納部２２内の価値実体１１ａから差し引かれ、該価値実体が、アドホックネットワークＮ２経由で店舗サーバ３０宛に送信される（Ｓ９）。かかる送信処理は、例えば、文献（「情報セキュリティ技術」2000年8月　社団法人電気通信協会発行　伊土誠一監修、松本隆明、岡本龍明編著）に記載されている既存の電子マネー送受信技術により実現可能である。

【００８１】

なお、商品又は役務の対価に相当する価値実体が価値実体１１ａよりも大きい場合には、価値実体送信部２７は、価値実体の減算及び送信を行わずに、残高が不足している旨のメッセージを表示装置２０ｄに表示させる。また、不足額分の価値実体がポストペイ（後払い）方式により補填されるものとしてもよい。

【００８２】

Ｓ１０では、携帯端末２０から送信された価値実体が、店舗サーバ３０の価値

実体受信部３３により受信される。

Ｓ１１では、店舗サーバ３０の領収書送信部３４により、商品又は役務の対価に相当する価値実体を受信した旨が電子的に表現されたデータ（領収書データ）が、アドホックネットワークＮ２経由で携帯端末２０宛に送信される。

【００８３】

Ｓ１２では、店舗サーバ３０から送信された領収書データが、携帯端末２０の領収書受信部２８により受信される。受信された領収書データは、アプリケーション３１ａにより、レンダリング可能な形式に変換され表示装置２０ｄに表示される。ここで、領収書の発行元を容易に識別可能とすると共に偽造を防止するために、コーヒーショップが選定した背景色を領収書データに使用したり、所定のアイコン（絵文字）を挿入してもよい。また、領収書の二重使用を予防するために、背景色やアイコンを所定の時間間隔で変更してもよい。更に、領収書データに、発行日時を示すタイムスタンプを入れてもよい。

【００８４】

コーヒーショップは、購入者である携帯端末２０のユーザに対して、領収書データを表示装置２０ｄに表示させることを求め、該領収書データの正当性を確認した後に、商品（上記例ではドライカフェラテ）を提供する。

【００８５】

なお、領収書は端末間で送受信されるとは限らない。すなわち、Ｓ１０において価値実体が受信されたことに伴い、その旨を知覚した店舗の店員が、該価値実体に相当する対価を受領した旨が表記された物理的な（紙媒体の）領収書を印刷出力し、ユーザに手渡すものとしても勿論よい。

【００８６】

Ｓ５における検証の結果、アプリケーションの電子署名が価値実体の提供元によって為されていないこと、又は、アプリケーションが改竄されていることが確認されると、アプリケーション検証部２４は、アプリケーションの検証に失敗したものと判断し（Ｓ６；Ｎｏ）、アプリケーション削除部２６に対して、アプリケーションの削除を指示する。

【００８７】

Ｓ１３では、Ｓ５で受信されたアプリケーションは、アプリケーション削除部２６により削除される。無線ＬＡＮを始めとするアドホックネットワークでは、通信事業者を介さずに端末装置間で直接的に通信が行われるので、通信内容が傍受されたり、コーヒーショップ以外の第三者が無線ＬＡＮによる別のサービスを近傍のエリアで提供したりすることが予見される。しかし、アプリケーションを削除することにより、悪意のある第三者により作成、又は改竄された可能性のあるアプリケーションを実行することに伴って生じる様々な危害が未然に防止される。その結果、電子購買支援システム１に関して高いセキュリティレベルを確保できる。

【００８８】

Ｓ１４では、Ｓ５で受信されたアプリケーションが削除された旨を示すメッセージが表示装置２０ｄに表示される。メッセージは、例えば、「取得したアプリケーションの検証に失敗しました。このため、アプリケーションを削除しました。」なるテキストデータである。これにより、携帯端末２０のユーザは、アプリケーションの検証に失敗した旨、及びアプリケーションが削除された旨を容易に認識できる。なお、アプリケーションの削除処理は、ユーザによる入力装置２０ｂからの指示を待って実行されるものとしてもよい。

【００８９】

以上説明した様に、第１の実施形態における電子購買支援システム１によれば、店舗サーバ３０から送信されたアプリケーションが必ずしも安全なものではない場合を懸念して、価値提供サーバ１０から事前に取得された価値実体に対する上記アプリケーションのアクセスを許可すべきか否かを検証する。かかる検証を行うための手段として、価値実体に予め添付された公開鍵と、アプリケーションの電子署名に使用された秘密鍵との作成元が一致するか否かを判定する。携帯端末２０は、検証が成功した場合にのみ、アプリケーションによる価値実体へのアクセスを許可し、当該アプリケーションを使用して店舗サーバ３０に価値実体を移転する。

【００９０】

これにより、提供元が保証されていないアプリケーションや改竄されたアプリ

ケーションが価値実体にアクセスすることが未然に防止され、価値実体が不正に使用されることがない。その結果、アドホックネットワークを使用して価値実体のやり取りを行う場合においても、安全かつ容易な電子購買支援が実現される。

【００９１】

（第２の実施の形態）

次に、本発明における第２の実施の形態について説明する。

第１の実施形態では、価値実体は、対応する公開鍵と共に、価値提供サーバ１０から携帯端末２０に送信されるものとしたが、本実施の形態では、価値実体と公開鍵とはそれぞれ個別に送信される。

【００９２】

本実施の形態における電子購買支援システムは、第１の実施形態において詳述した電子購買支援システム１と機能的構成を同様とする。また、本実施の形態における携帯端末は、上述した携帯端末２０とハードウェア構成を同一とする。したがって、共通する構成要素には同一の符合を付し、その説明は省略すると共に、第１の実施の形態との差異について詳述する。

【００９３】

以下、図７を参照して、第２の実施形態における電子購買支援システムにより実行される電子購買処理について説明する。

本実施の形態における電子購買処理は、第１の実施形態において詳述した電子購買処理（図４参照）と共通するステップを複数含む。具体的には、図７のＳ２５～Ｓ３６の各ステップは、図４に示したＳ３～Ｓ１４の各ステップにそれぞれ相当する。

【００９４】

以下、本実施の形態に特有のステップであるＳ２１～Ｓ２４（図７中の太線で囲んだ処理）について説明する。まず、Ｓ２１では、携帯端末２０のユーザが、ペイメントサービスプロバイダと商品又は役務の売買に関する契約を締結したこと、又は、該プロバイダへのアカウントを作成したことに伴い、価値提供サーバ１０の価値実体送信部１２により、公開鍵Ａ１が、セルラーネットワークＮ１及び基地局Ｂ経由で携帯端末２０宛に送信される。

【００９５】

Ｓ２２では、Ｓ２１で送信された公開鍵Ａ１が、携帯端末２０の価値実体受信部２１により受信され価値実体格納部２２に格納される。なお、公開鍵Ａ１は、携帯端末２０の製造時等に、記憶装置２０ｅに予め格納しておくものとしてもよい。

【００９６】

Ｓ２３では、携帯端末２０のユーザが、クレジットカードによる電子決済や通信事業者による代行課金などの商取引により価値実体を購入する。これに伴い、価値提供サーバ１０の価値実体送信部１２により、公開鍵Ａ１に対応する価値実体１１ａが、セルラーネットワークＮ１及び基地局Ｂ経由で携帯端末２０宛に送信される。

【００９７】

Ｓ２４では、Ｓ２３で送信された価値実体１１ａが、携帯端末２０の価値実体受信部２１により受信され、公開鍵Ａ１及びサービス識別子と対応付けて、価値実体格納部２２に格納される。

その後、Ｓ２５以降の処理が実行されるが、Ｓ２５～Ｓ３６の各ステップは、第１の実施形態におけるＳ３～Ｓ１４（図４参照）の各ステップと同一であるので、その説明は省略する。

【００９８】

第２の実施形態における電子購買支援システムによれば、Ｓ２３及びＳ２４の処理を繰り返し実行することにより、携帯端末２０への価値実体の補充（チャージ）が可能となる。すなわち、携帯端末２０が価値実体を受信した時点で、価値実体格納部２２に価値実体が残存する場合には、該価値実体の額と、受信された価値実体の額とが加算（マージ）される。この際、価値提供サーバ１０は、送信する価値実体に公開鍵を添付する必要がないので、電子購買処理に伴う通信データ量を低減することができる。

【００９９】

（第３の実施の形態）

次に、本発明における第３の実施の形態について説明する。

第１及び第２の実施形態では、携帯端末２０は、価値提供サーバ１０から予め取得した公開鍵を、対応する価値実体と共に価値実体格納部２２に格納し、常時保持するものとした。これに対して、本実施の形態では、携帯端末２０は、アプリケーションを使用して電子購買を行う都度、価値提供サーバ１０に公開鍵の送信を要求して取得する。

【０１００】

図８は、本実施の形態における電子購買支援システム２の機能的構成を示すシステム構成図である。電子購買支援システム２は、第１及び第２の実施形態における電子購買支援システム１と機能的に共通する構成要素を複数含む。また、本実施の形態における携帯端末は、上述した携帯端末２０とハードウェア構成を同一とする。したがって、共通の構成要素には同一の符号を付し、その説明は省略すると共に、上記各実施の形態との差異について詳述する。

【０１０１】

図８に示すように、価値提供サーバ１０は、機能的には、価値実体格納部１１と公開鍵公開部１３と価値実体送信部１２と公開鍵送信部１４とを有する。

価値実体格納部１１には、店舗における商品又は役務の電子購買に使用される価値実体１１ｂが格納されている。

公開鍵公開部１３は、アプリケーション３１ａの起動に必要な公開鍵Ａ１を更新可能に保持する。公開鍵公開部１３は、携帯端末２０を含む複数の携帯端末がセルラーネットワークＮ１を経由してアクセス可能な形態で公開鍵Ａ１を公開する。

【０１０２】

価値実体送信部１２は、携帯端末２０からの価値実体送信要求に応じて、価値実体１１ｂを価値実体格納部１１から読み出し、セルラーネットワークＮ１及び基地局Ｂを介して携帯端末２０宛に送信する。

公開鍵送信部１４は、携帯端末２０からの公開鍵送信要求に応じて、公開鍵Ａ１を公開鍵公開部１３から取得し、セルラーネットワークＮ１及び基地局Ｂを介して携帯端末２０宛に送信する。

【０１０３】

図８に示すように、携帯端末２０は、機能的には、価値実体受信部２１と、価値実体格納部２２と、アプリケーション受信部２３と、公開鍵送信要求部２９と、公開鍵受信部２１０と、アプリケーション検証部２４と、アプリケーション起動部２５と、アプリケーション削除部２６と、価値実体送信部２７と、領収書受信部２８とを有する。

【０１０４】

公開鍵送信要求部２９は、アプリケーション受信部２３によるアプリケーション３１ａの受信に伴って、アプリケーション３１ａの起動に必要な公開鍵（公開鍵Ａ１）の送信を、価値提供サーバ１０に対して要求する。

公開鍵受信部２１０は、価値提供サーバ１０の公開鍵送信部１４により送信された公開鍵Ａ１を受信し、公開鍵Ａ１を使用してアプリケーション３１ａを検証することをアプリケーション検証部２４に指示する。

【０１０５】

以下、図９を参照して、第３の実施形態における電子購買支援システムにより実行される電子購買処理について説明する。

本実施の形態における電子購買処理は、第１の実施形態において詳述した電子購買処理（図４参照）と共通するステップを複数含む。具体的には、図９のＳ４４，Ｓ４５，Ｓ４９～Ｓ５７の各ステップは、図４に示したＳ３，Ｓ４，Ｓ６～Ｓ１４の各ステップにそれぞれ相当する。

【０１０６】

以下、本実施の形態に特有のステップであるＳ４１～Ｓ４３，Ｓ４６，Ｓ４７（図９中の太線で囲んだ処理）について説明する。まず、Ｓ４１では、価値提供サーバ１０の公開鍵公開部１３により、公開鍵Ａ１が、携帯端末２０からセルラーネットワークＮ１を経由してアクセスが可能な形態で公開される。

【０１０７】

Ｓ４２では、携帯端末２０のユーザが、クレジットカードによる電子決済や通信事業者による代行課金などの商取引により価値実体を購入する。これに伴い、価値提供サーバ１０の価値実体送信部１２により、公開鍵Ａ１に対応する価値実体１１ａが、セルラーネットワークＮ１及び基地局Ｂ経由で携帯端末２０宛に送

信される。

【０１０８】

Ｓ４３では、Ｓ４２で送信された価値実体１１ａが、携帯端末２０の価値実体受信部２１により受信され、サービス識別子と対応付けて、価値実体格納部２２に格納される。この時点では、公開鍵Ａ１は、携帯端末２０に存在しない。

【０１０９】

携帯端末２０が、アドホックネットワークＮ２により店舗サーバ３０に接続されると（Ｓ４４）、店舗サーバ３０からアドホックネットワークＮ２を経由して携帯端末２０宛にアプリケーション３１ａが送信される（Ｓ４５）。

Ｓ４６では、アプリケーション３１ａの受信を契機として、公開鍵送信要求部２９により、アプリケーション３１ａの起動に必要な公開鍵Ａ１の送信要求が、価値提供サーバ１０宛に送信される。この送信要求は、秘匿性及び安全性の高いセルラーネットワークＮ１を経由して送信される。

【０１１０】

Ｓ４７では、Ｓ４６で送信された公開鍵送信要求に応じて、公開鍵送信部１４により、公開鍵公開部１３から公開鍵Ａ１が取得され、セルラーネットワークＮ１経由で携帯端末２０宛に送信される。

【０１１１】

Ｓ４７で送信された公開鍵Ａ１は、携帯端末２０の公開鍵受信部２１０により受信される（Ｓ４８）。公開鍵Ａ１の受信に伴い、携帯端末２０は、アプリケーション検証部２４により、Ｓ４６で受信されたアプリケーション３１ａの検証を開始する。その後、Ｓ４９以降の処理が実行されるが、Ｓ４９～Ｓ５７の各ステップは、第１の実施形態におけるＳ６～Ｓ１４（図４参照）の各ステップと同一であるので、その説明は省略する。

【０１１２】

第３の実施形態における電子購買支援システム２によれば、ペイメントサービスプロバイダが価値提供サーバ１０上に公開鍵Ａ１を公開しておくことにより、携帯端末２０は、公開鍵Ａ１を常時保持していなくとも、必要に応じて、価値提供サーバ１０から公開鍵Ａ１を取得することができる。したがって、携帯端末２

０のデータ記憶容量を節約できる。

【０１１３】

また、秘密鍵Ａ２を適宜更新することは、電子購買支援の安全性向上に資するが、秘密鍵Ａ２の更新に遅滞なく、携帯端末２０の保持する公開鍵Ａ１を更新することは困難である。そこで、電子購買支援システム２では、携帯端末２０が、アプリケーション３１ａを受信する度に公開鍵Ａ１を能動的に取得する。これにより、携帯端末２０のユーザは、秘密鍵Ａ２が更新された場合でも、最新の秘密鍵Ａ２に対応する公開鍵Ａ１を確実かつ容易に入手することができる。その結果、電子購買支援システム２は、高いセキュリティを維持しつつ、容易な電子購買を提供できる。

【０１１４】

（第４の実施の形態）

次に、本発明における第４の実施の形態について説明する。

第１～第３の実施形態では、携帯端末２０は、受信したアプリケーションの検証に失敗した時に、該アプリケーションを削除するものとした。これに対して、本実施の形態では、携帯端末２０は、アプリケーションを受信した時点から所定時間が経過したことを契機として自動的にアプリケーションを削除する。以下、第１の実施形態における電子購買支援システム１に経過時間測定機能を付加した電子購買支援システム３について代表的に説明するが、第２及び第３の実施形態における電子購買支援システムに関しても本機能を適用することは可能である。

【０１１５】

図１０は、本実施の形態における電子購買支援システム３の機能的構成を示すシステム構成図である。電子購買支援システム３は、第１の実施形態における電子購買支援システム１と機能的に共通する構成要素を複数含む。また、本実施の形態における携帯端末は、上述した携帯端末２０とハードウェア構成を同一とする。したがって、共通の構成要素には同一の符号を付し、その説明は省略すると共に、第１の実施形態との差異について詳述する。

【０１１６】

店舗サーバ３０から携帯端末２０に送信されるアプリケーション３１ａには、

店舗によって任意に設定された所定時間Ｔ１（例えば１～３時間程度）が予め記述されている。

図１０に示すように、携帯端末２０は、機能的には、価値実体受信部２１と、価値実体格納部２２と、アプリケーション受信部２３と、経過時間測定部２１１と、アプリケーション検証部２４と、アプリケーション起動部２５と、アプリケーション削除部２６と、価値実体送信部２７と、領収書受信部２８とを有する。

【０１１７】

経過時間測定部２１１は、アプリケーション受信部２３によりアプリケーション３１ａが受信された時点で、経過時間の測定を開始する。同時に、経過時間測定部２１１は、アプリケーション３１ａから所定時間Ｔ１を取得し、上記経過時間が所定時間Ｔ１に到達するのを待機する。経過時間測定部２１１は、上記経過時間が所定時間Ｔ１に到達したことを契機として、アプリケーション削除部２６に対し、アプリケーション３１ａの削除を指示する。

【０１１８】

アプリケーション削除部２６は、経過時間測定部２１１からの指示に応じて、アプリケーション３１ａを削除する。なお、アプリケーション３１ａにより作成されたファイルがあれば、アプリケーション削除部２６は、これも削除する。該ファイルとは、例えば、レンダリング可能な形式に変換された領収書データである。

【０１１９】

第４の実施形態における電子購買支援システム３によれば、アプリケーション３１ａは、携帯端末２０により受信された時点からの所定時間の経過に伴い、自動的に削除される。これにより、アプリケーション３１ａは、携帯端末２０内に所定時間を超えて留まることがない。したがって、アプリケーション３１ａ又はこれにより作成されたファイルが、別の店舗で使用され、電子商取引に混乱が生じる恐れを回避できる。

【０１２０】

更に、第４の実施形態の変形態様として、携帯端末２０は、アプリケーション３１ａを受信した後も店舗サーバ３０との間に通信セッションを継続すると共に

、経過時間測定部２１１は、該通信セッションが切断された時点で、経過時間の測定を開始するものとしてもよい。この場合においても、経過時間測定部２１１は、計時開始と同時に、アプリケーション３１ａから所定時間Ｔ２（例えば５分程度）を取得し、上記経過時間が所定時間Ｔ２に到達するのを待機する。経過時間測定部２１１は、上記経過時間が所定時間Ｔ２に到達したことを契機として、アプリケーション削除部２６に対し、アプリケーション３１ａの削除を指示する。

【０１２１】

アプリケーション削除部２６は、経過時間測定部２１１からの指示に応じて、アプリケーション３１ａを削除する。なお、アプリケーション３１ａにより作成されたファイルがあれば、アプリケーション削除部２６はこれも削除する。該ファイルとは、例えば、レンダリング可能な形式に変換された領収書データである。

【０１２２】

通信セッションの切断は、アドホックネットワークＮ２の通信圏内から携帯端末２０が離れる等の外的要因により生じる。本変形態様における電子購買支援システムによれば、アプリケーション３１ａは、通信セッションの切断を契機として削除される。換言すれば、アプリケーション３１ａが保持される時間は、通信セッションの継続時間に依存することになり、携帯端末２０のユーザが店舗から退出したことに起因して、アプリケーション３１ａは、迅速かつ確実に携帯端末２０から削除される。したがって、アプリケーション３１ａが別の店舗で使用され、電子商取引に混乱が生じる懸念を解消できる。

【０１２３】

また、通信環境によっては、アプリケーション３１ａの受信完了後かつ検証完了前に何らかの要因により通信が切断され、検証処理を経ていないアプリケーション３１ａが携帯端末２０に残る可能性がある。そこで、かかる場合には、アプリケーション削除部２６は、所定時間の経過を待ってアプリケーション３１ａを自動的に削除することにより、正当性が保証されていないアプリケーションが携帯端末２０に保持されることを未然に防止できる。所定時間は、アプリケーショ

ン３１ａの受信直後に当該アプリケーションが価値実体の移転に使用される事態を回避する観点から、充分に短い時間（例えば１～３秒程度）であることが望ましい。

【０１２４】

（第５の実施の形態）

次に、本発明における第５の実施の形態について説明する。

本実施の形態では、携帯端末は、想定された通りに正常に動作するか否かを示す指標であるインテグリティを測定する機能を有する。価値提供サーバは、携帯端末から送信された測定結果を検証し、検証に成功した場合にのみ、携帯端末宛に価値実体を送信する。同様に、店舗サーバは、上記測定結果の検証に成功した場合にのみ、携帯端末宛にアプリケーションを送信する。

【０１２５】

以下、第１の実施形態における電子購買支援システム１の携帯端末２０にインテグリティ測定機能を付加した電子購買支援システム４について代表的に説明するが、第２～第４の実施形態における電子購買支援システムに関しても本機能を適用することは可能である。

【０１２６】

図１１は、本実施の形態における電子購買支援システム４の機能的構成を示すシステム構成図である。電子購買支援システム４は、第１の実施形態における電子購買支援システム１と機能的に共通する構成要素を複数含む。また、本実施の形態における携帯端末は、上述した携帯端末２０とハードウェア構成を同一とする。したがって、共通の構成要素には同一の符号を付し、その説明は省略すると共に、第１の実施形態との差異について詳述する。

【０１２７】

図１１に示すように、価値提供サーバ１０は、機能的には、価値実体格納部１１と、測定結果送信要求部１５と、測定結果受信部１６と、測定結果検証部１７（第２検証手段に対応）と、価値実体送信部１２とを有する。測定結果送信要求部１５は、携帯端末２０に対して、インテグリティの測定結果の送信を要求する。測定結果受信部１６は、携帯端末２０の測定結果送信部２１３により送信され

た上記測定結果をセルラーネットワークＮ１経由で受信する。

【０１２８】

測定結果検証部１７は、測定結果受信部１６により受信された上記測定結果を検証し、携帯端末２０における信頼性の有無を判定する。インテグリティ測定結果の検証処理に関しては、例えば、文献（Compaq Computer Corporation, Hewlett-Packard Company, IBM Corporation, Intel Corporation, Microsoft Corporation,「Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1b」, 22 February 2002、http://www.trustedcomputing.org/docs/main%20v1_1b.pdf）に記載されている既存の技術により実現可能である。

【０１２９】

携帯端末２０は、機能的には、インテグリティ測定部２１２と、測定結果送信部２１３と、価値実体受信部２１と、価値実体格納部２２と、アプリケーション受信部２３と、アプリケーション検証部２４と、アプリケーション起動部２５と、アプリケーション削除部２６と、価値実体送信部２７と、領収書受信部２８とを有する。

【０１３０】

インテグリティ測定部２１２は、既存技術であるＴＰＭ（Trusted Platform Module）が携帯端末２０の制御装置２０ａにより実行されることにより実現する機能を有し、携帯端末２０のインテグリティを測定する。インテグリティの測定処理に関しても、例えば、上記文献に記載の技術により実現可能である。

【０１３１】

測定結果送信部２１３は、インテグリティ測定部２１２によるインテグリティ測定結果を価値提供サーバ１０宛に送信する。

【０１３２】

店舗サーバ３０は、機能的には、アプリケーション格納部３１と、測定結果送信要求部３５と、測定結果受信部３６と、測定結果検証部３７（第３検証手段に対応）と、アプリケーション送信部３２と、価値実体受信部３３と、領収書送信部３４とを有する。測定結果送信要求部３５は、携帯端末２０に対して、インテグリティの測定結果の送信を要求する。測定結果受信部３６は、携帯端末２０の

測定結果送信部２１３により送信された上記測定結果をアドホックネットワークＮ２経由で受信する。測定結果検証部３７は、測定結果受信部３６により受信された上記測定結果を検証し、携帯端末２０における信頼性の有無を判定する。

【０１３３】

以下、図１２を参照して、第５の実施形態における電子購買支援システムにより実行される電子購買処理について説明する。

本実施の形態における電子購買処理は、第１の実施形態において詳述した電子購買処理（図４参照）と共通するステップを複数含む。具体的には、図１２のＳ６６～Ｓ６８，Ｓ７４～Ｓ７６の各ステップは、図１２に示したＳ１～Ｓ３，Ｓ４～Ｓ６の各ステップにそれぞれ相当する。Ｓ７６の後処理に関しては図示しないが、図４に示したＳ７以降の処理と同一の処理が実行される。

【０１３４】

以下、本実施の形態に特有のステップであるＳ６１～Ｓ６５，Ｓ６９～Ｓ７３（図１２中の太線で囲んだ処理）について説明する。まず、Ｓ６１では、価値提供サーバ１０の公開鍵公開部１３により、公開鍵Ａ１が、携帯端末２０からセルラーネットワークＮ１を経由してアクセスが可能な形態で公開される。

【０１３５】

Ｓ６１では、価値提供サーバ１０が携帯端末２０の信頼性を確認すべく、価値提供サーバ１０の測定結果送信要求部１５により、インテグリティの送信要求が携帯端末２０宛に送信される。この送信要求は、秘匿性及び安全性の高いセルラーネットワークＮ１を経由して送信される。

【０１３６】

Ｓ６２では、Ｓ６１にて送信された送信要求に応じて、インテグリティ測定部２１２により、携帯端末２０のインテグリティが測定される。

Ｓ６３では、Ｓ６２にて測定されたインテグリティが、測定結果送信部２１３により、セルラーネットワークＮ１経由で価値提供サーバ１０宛に送信される。

【０１３７】

Ｓ６４では、Ｓ６３にて携帯端末２０から送信されたインテグリティ測定結果が測定結果受信部１６により受信され、測定結果検証部１７により該測定結果が

検証される。検証の結果、インテグリティの検証に成功した場合には（Ｓ６５；Ｙｅｓ）、Ｓ６６に進み、公開鍵Ａ１が添付された価値実体１１ａが、セルラーネットワークＮ１及び基地局Ｂ経由で携帯端末２０宛に送信される。

【０１３８】

Ｓ６４における検証の結果、インテグリティの検証に失敗した場合には（Ｓ６５；Ｎｏ）、一連の電子購買処理を終了する。インテグリティの検証に失敗する要因としては、例えば、携帯端末２０がウイルスに感染している等の理由により信頼できない状態にある場合が挙げられる。

【０１３９】

携帯端末２０と店舗サーバ３０とが接続されると（Ｓ６８）、Ｓ６９では、店舗サーバ３０が携帯端末２０の信頼性を確認すべく、店舗サーバ３０の測定結果送信要求部３５により、インテグリティの送信要求が携帯端末２０宛に送信される。

【０１４０】

Ｓ７０では、Ｓ６９にて送信された送信要求に応じて、インテグリティ測定部２１２により、携帯端末２０のインテグリティが測定される。

Ｓ７１では、Ｓ７０にて測定されたインテグリティが、測定結果送信部２１３により、アドホックネットワークＮ２経由で店舗サーバ３０宛に送信される。

【０１４１】

Ｓ７２では、Ｓ７１にて携帯端末２０から送信されたインテグリティ測定結果が測定結果受信部３６により受信され、測定結果検証部３７により当該測定結果が検証される。検証の結果、インテグリティの検証に成功した場合には（Ｓ７３；Ｙｅｓ）、Ｓ７４に進み、アプリケーション格納部３１内のアプリケーション３１ａが、アドホックネットワークＮ２経由で携帯端末２０宛に送信される。一方、インテグリティの検証に失敗した場合には（Ｓ７３；Ｎｏ）、一連の電子購買処理を終了する。

【０１４２】

第５の実施形態における電子購買支援システム４によれば、価値提供サーバ１０は、価値実体を送信する前に、その送信先である携帯端末２０のインテグリテ

ィ測定結果を取得し、この測定結果に基づいて携帯端末２０の信頼性の有無を判定する。そして、信頼性があると判断された携帯端末に対してのみ価値実体を送信する。したがって、ウイルス感染や悪意による改造の可能性のある携帯端末が価値実体を取得することに起因して、電子購買支援システムに危害が及び、信頼性が低下することを未然に防止できる。

【０１４３】

また、第５の実施形態における電子購買支援システム４によれば、店舗サーバ３０は、アプリケーションを送信する前に、その送信先である携帯端末２０のインテグリティ測定結果を取得し、この測定結果に基づいて携帯端末２０の信頼性の有無を判定する。そして、信頼性があると判断された携帯端末に対してのみアプリケーションを送信する。これにより、携帯端末２０のインテグリティは、価値実体の受信直前に限らず、アプリケーションの受信直前にも再び検証されることになる。したがって、例えば、携帯端末２０が価値実体を受信した時点ではインテグリティに問題はなかったが受信後にインテグリティが低下した場合などに、携帯端末２０が不適切に振る舞って、電子購買支援システムに危害が及び、信頼性が低下することを回避できる。

【０１４４】

最後に、上述した一連の電子購買処理を携帯端末２０に実行させるための電子購買支援プログラムについて説明する。図１３に示すように、電子購買支援プログラム４１は、記録媒体４０に形成されたプログラム格納領域４０ａ内に格納されている。

【０１４５】

電子購買支援プログラム４１は、電子購買処理を統括的に制御するメインモジュール４１ａと、外部から送信された価値実体を受信する処理を携帯端末２０に実行させる価値実体受信モジュール４１ｂと、受信された価値実体をメモリ等の格納手段に格納する処理を携帯端末２０に実行させる価値実体格納モジュール４１ｃと、外部から送信されたアプリケーションを受信する処理を携帯端末２０に実行させるアプリケーション受信モジュール４１ｄと、受信されたアプリケーションを検証する処理を携帯端末２０に実行させるアプリケーション検証モジュー

ル４１ｅと、検証に成功したアプリケーションを起動する処理を携帯端末２０に実行させるアプリケーション起動モジュール４１ｆと、検証に失敗したアプリケーションを削除する処理を携帯端末２０に実行させるアプリケーション削除モジュール４１ｇと、アプリケーションの送信元宛に価値実体を送信する処理を携帯端末２０に実行させる価値実体送信モジュール４１ｈと、外部から送信された、価値実体に対する領収書データを受信する処理を携帯端末２０に実行させる領収書受信モジュール４１ｉとを備えて構成される。

【０１４６】

価値実体受信モジュール４１ｂと、アプリケーション受信モジュール４１ｄと、アプリケーション検証モジュール４１ｅと、アプリケーション起動モジュール４１ｆと、アプリケーション削除モジュール４１ｇと、価値実体送信モジュール４１ｈと、領収書受信モジュール４１ｉの各モジュールを実行させることによって実現する機能は、携帯端末２０の有する価値実体受信部２１と、アプリケーション受信部２３と、アプリケーション検証部２４と、アプリケーション起動部２５と、アプリケーション削除部２６と、価値実体送信部２７と、領収書受信部２８の機能と同様である。また、価値実体格納モジュール４１ｃを実行させることによって格納されるデータは、価値実体格納部２２に格納されるデータと同様である。

【０１４７】

電子購買支援プログラム４１は、その一部若しくは全部が、通信回線等の伝送媒体を介して伝送され、他の機器により受信されて記録（インストールを含む）される構成としてもよい。

【０１４８】

【発明の効果】

本発明によれば、アドホックネットワークを経由して取得されたアプリケーションを使用して、安全かつ容易に価値実体の授受を行うことが可能となる。

【図面の簡単な説明】

【図１】

電子購買支援システムの全体構成を概念的に示す図である。

【図２】

第１及び第２の実施形態における電子購買支援システムの機能的構成を示す図である。

【図３】

携帯端末のハードウェア構成を示すブロック図である。

【図４】

第１の実施形態における電子購買支援システムによって実行される電子購買処理の流れを示すフローチャートである。

【図５】

複数種の価値実体が格納されている場合における価値実体格納部のデータ格納例を示す図である。

【図６】

電子購買処理の実行に際して、携帯端末の表示装置に表示される商品メニューの一例を示す図である。

【図７】

第２の実施形態における電子購買支援システムによって実行される電子購買処理の流れを示すフローチャートである。

【図８】

第３の実施形態における電子購買支援システムの機能的構成を示す図である。

【図９】

第３の実施形態における電子購買支援システムによって実行される電子購買処理の流れを示すフローチャートである。

【図１０】

第４の実施形態の変形態様における電子購買支援システムの機能的構成を示す図である。

【図１１】

第５の実施形態における電子購買支援システムの機能的構成を示す図である。

【図１２】

第５の実施形態における電子購買支援システムによって実行される電子購買処

理の流れを示すフローチャートである。

【図１３】

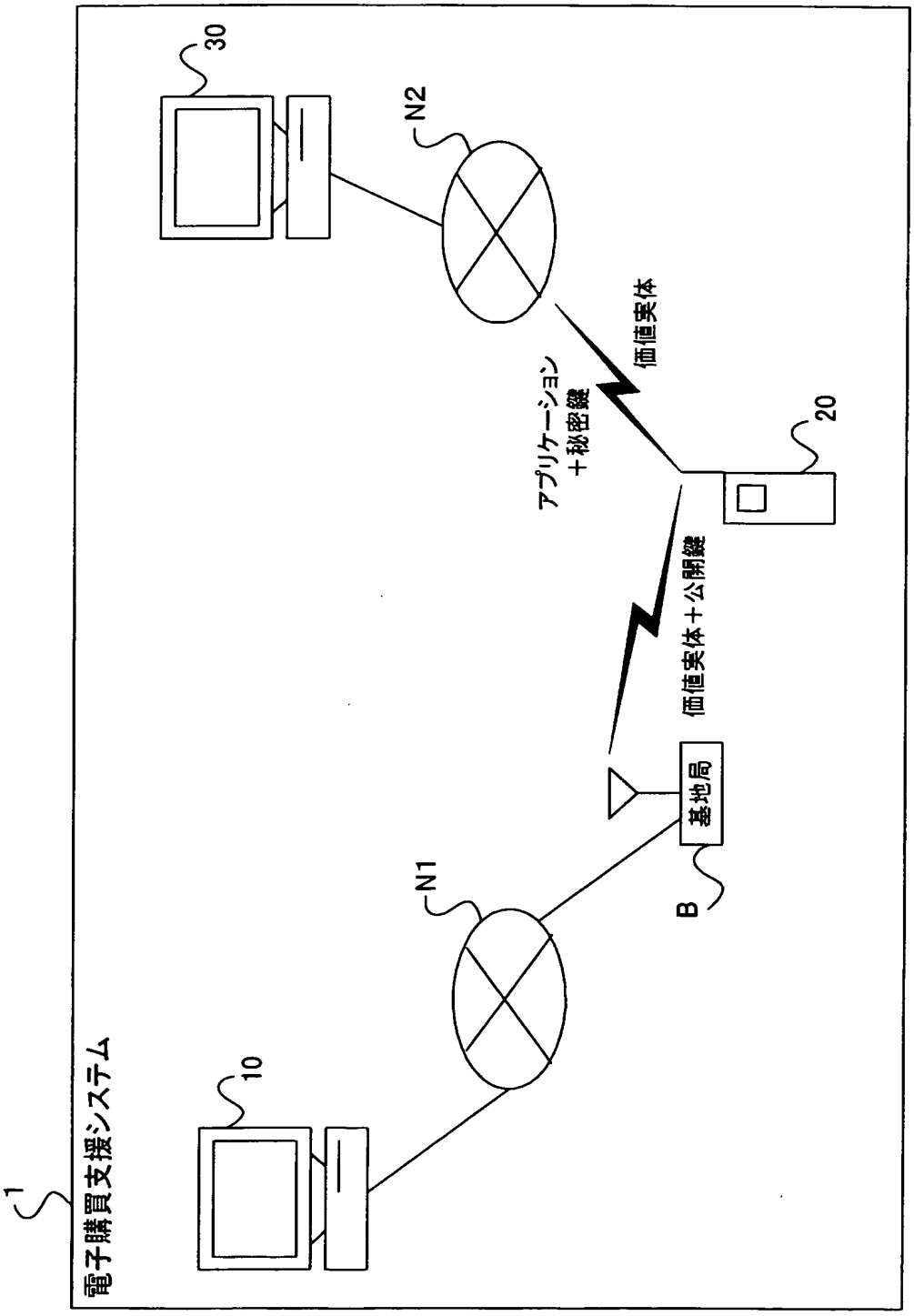
本発明に係る電子購買支援プログラムの構成を示す図である。

【符号の説明】

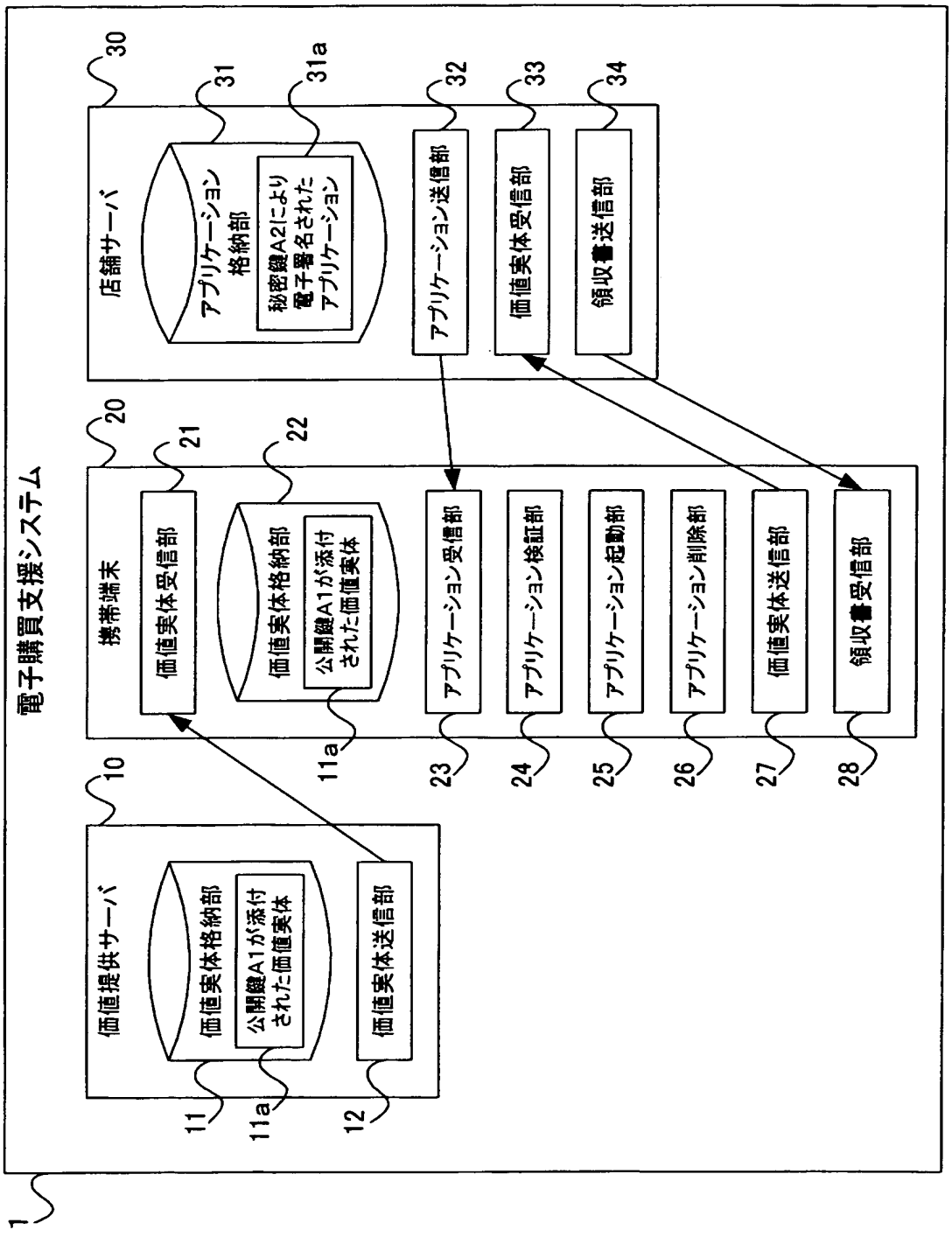
１…電子購買支援システム、１０…価値提供サーバ、１１…価値実体格納部、１１ａ…価値実体、１２…価値実体送信部、１３…公開鍵公開部、１４…公開鍵送信部、１５…測定結果送信要求部、１６…測定結果受信部、１７…測定結果検証部、２１２…インテグリティ測定部、２１３…測定結果送信部、３５…測定結果送信要求部、３６…測定結果受信部、３７…測定結果検証部、２１２…インテグリティ測定部、２０…携帯端末、２１…価値実体受信部、２２…価値実体格納部、２３…アプリケーション受信部、２４…アプリケーション検証部、２５…アプリケーション起動部、２６…アプリケーション削除部、２７…価値実体送信部、２８…領収書受信部、２９…公開鍵送信要求部、２１０…公開鍵受信部、２１１…経過時間測定部、３０…店舗サーバ、３１…アプリケーション格納部、３１ａ…アプリケーション、３２…アプリケーション送信部、３３…価値実体受信部、３４…領収書送信部、Ａ１…公開鍵、Ａ２…秘密鍵

【書類名】　　図面

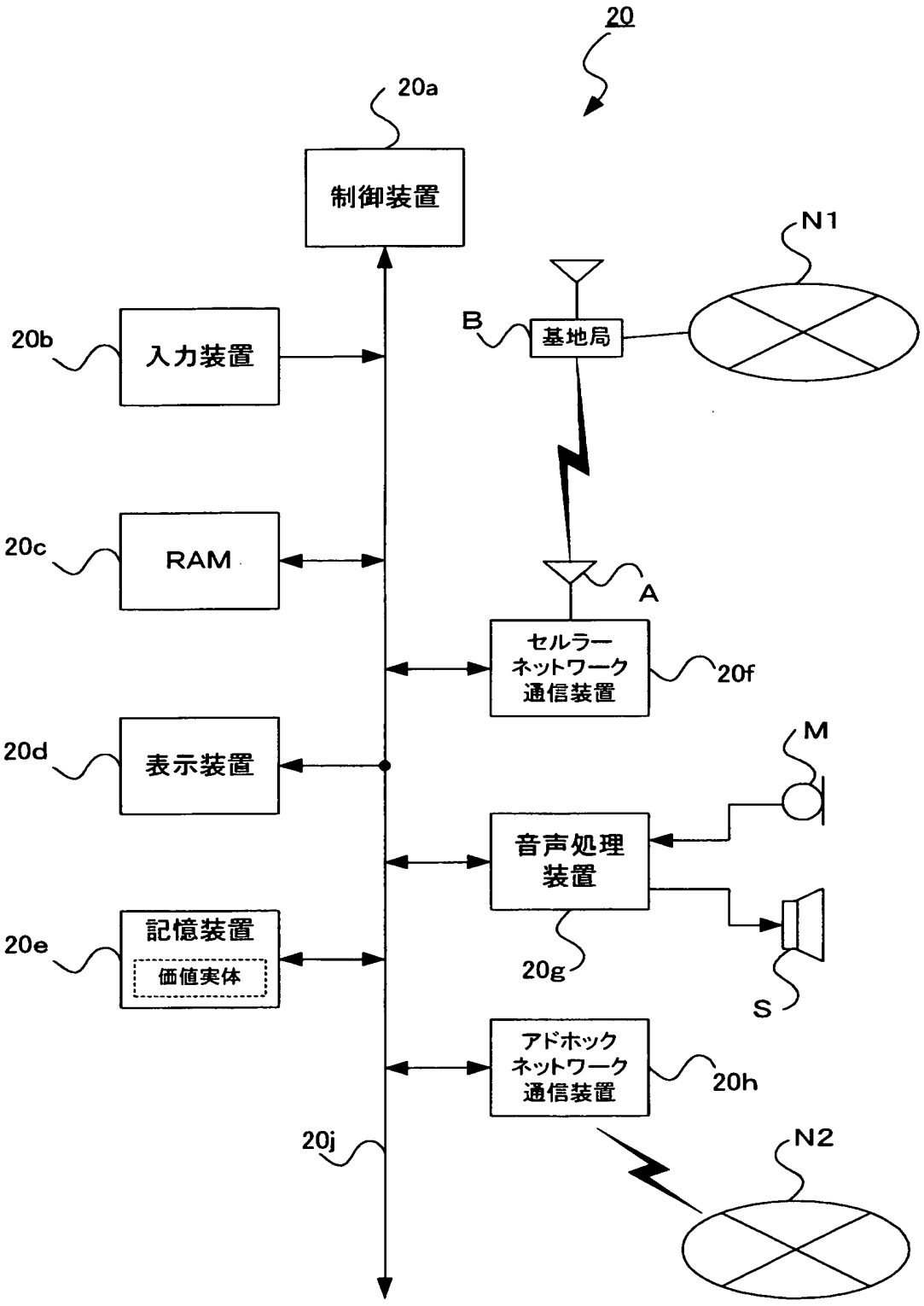
【図１】



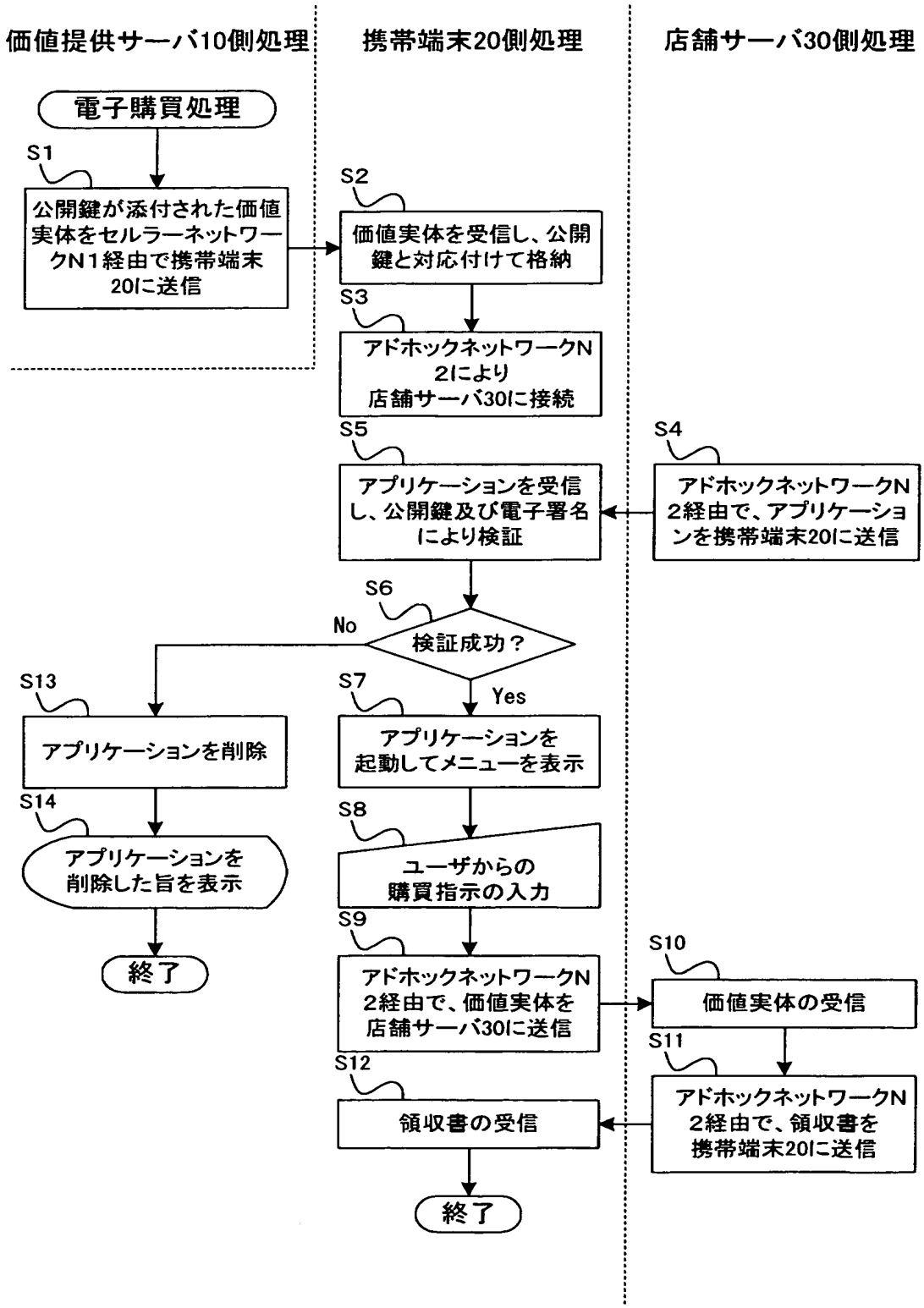
【図２】


電子購買支援システム
1
店舗サーバ
30
アプリケーション格納部
31
秘密鍵A2により電子署名されたアプリケーション
31a
アプリケーション送信部
32
価値実体受信部
33
領収書送信部
34
携帯端末
20
価値実体受信部
21
価値実体格納部
22
公開鍵A1が添付された価値実体
11a
アプリケーション受信部
23
アプリケーション検証部
24
アプリケーション起動部
25
アプリケーション削除部
26
価値実体送信部
27
領収書受信部
28
価値提供サーバ
10
価値実体格納部
11
公開鍵A1が添付された価値実体
11a
価値実体送信部
12

【図３】


20
20a
制御装置
N1
B
基地局
20b
入力装置
20c
RAM
A
セルラー
ネットワーク
通信装置
20f
20d
表示装置
M
音声処理
装置
20e
記憶装置
価値実体
20g
S
アドホック
ネットワーク
通信装置
20h
20j
N2

【図４】

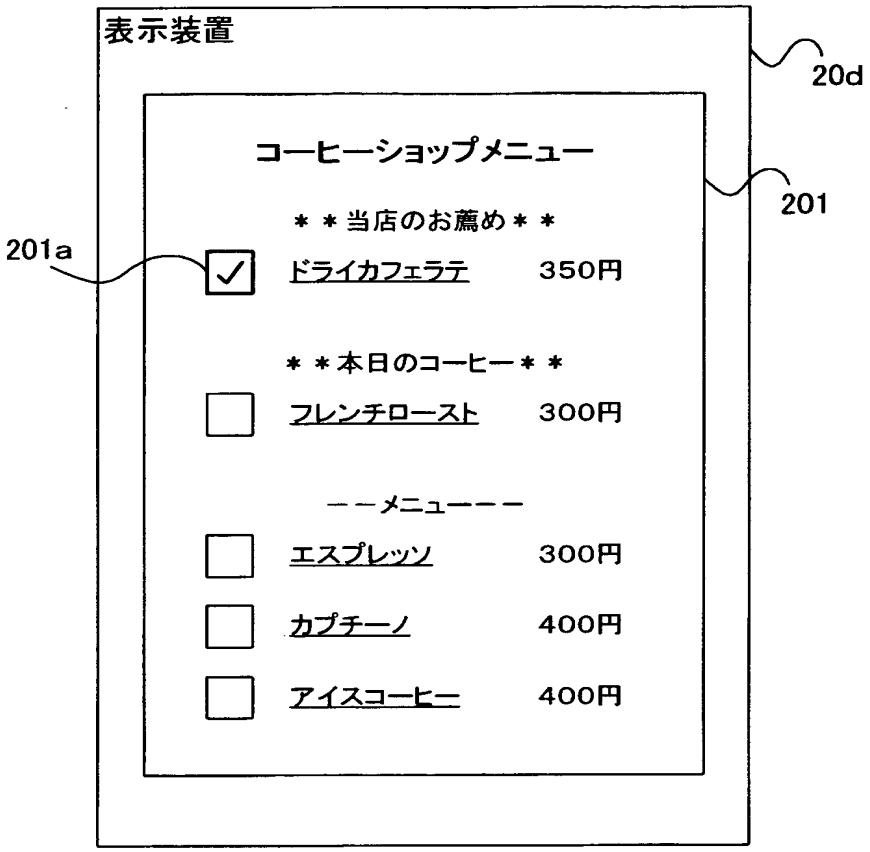

価値提供サーバ10側処理
携帯端末20側処理
店舗サーバ30側処理
電子購買処理
S1
公開鍵が添付された価値実体をセルラーネットワークN1経由で携帯端末20に送信
S2
価値実体を受信し、公開鍵と対応付けて格納
S3
アドホックネットワークN2により店舗サーバ30に接続
S4
アドホックネットワークN2経由で、アプリケーションを携帯端末20に送信
S5
アプリケーションを受信し、公開鍵及び電子署名により検証
S6
検証成功？
No
Yes
S7
アプリケーションを起動してメニューを表示
S8
ユーザからの購買指示の入力
S9
アドホックネットワークN2経由で、価値実体を店舗サーバ30に送信
S10
価値実体の受信
S11
アドホックネットワークN2経由で、領収書を携帯端末20に送信
S12
領収書の受信
終了
S13
アプリケーションを削除
S14
アプリケーションを削除した旨を表示
終了

【図５】

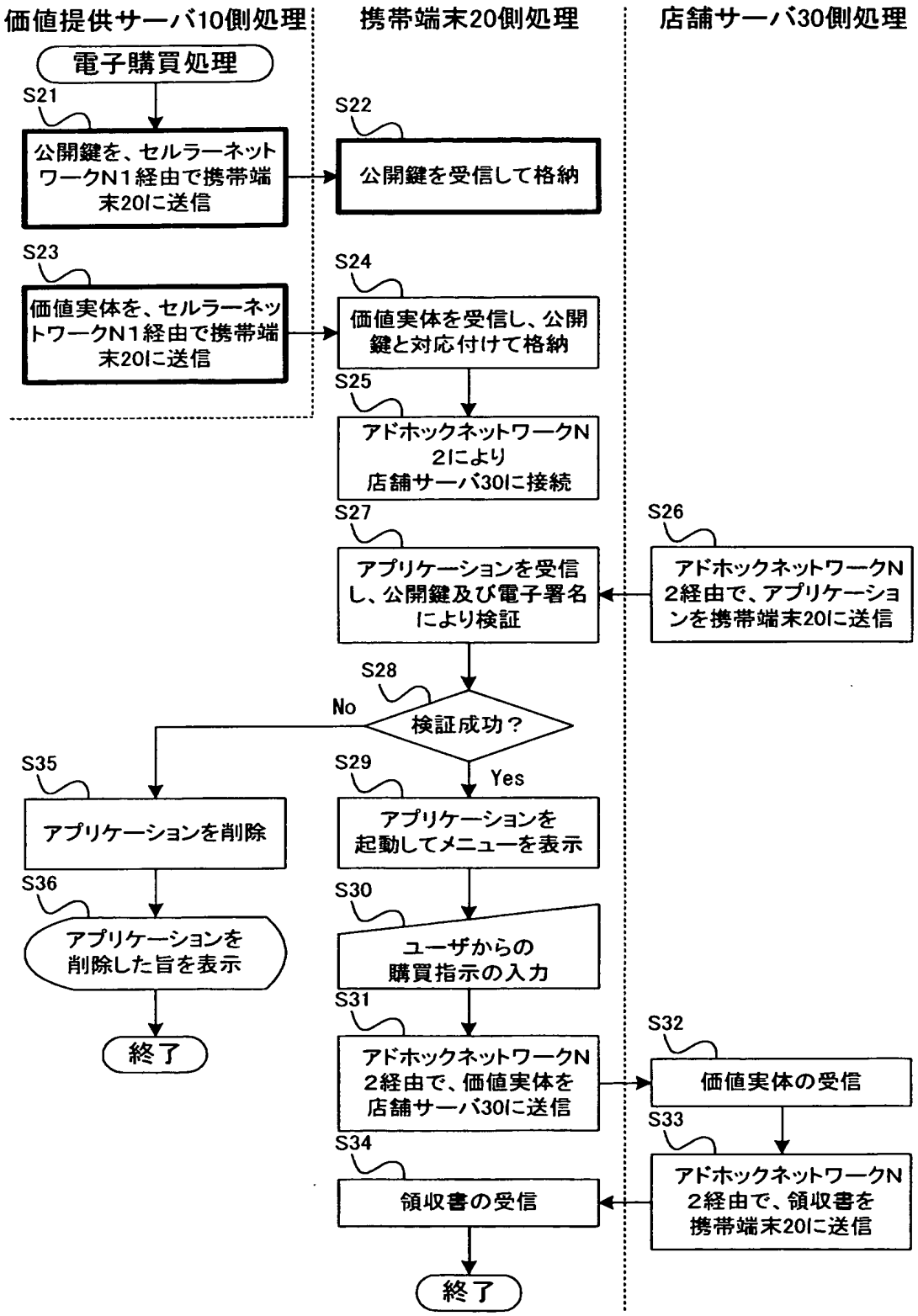
221　222

価値実体領域	サービス識別子領域
公開鍵A1が添付された価値実体11a	0001
公開鍵A2が添付された価値実体	0001
公開鍵A3が添付された価値実体	0002
公開鍵A4が添付された価値実体	0003
⋮	⋮

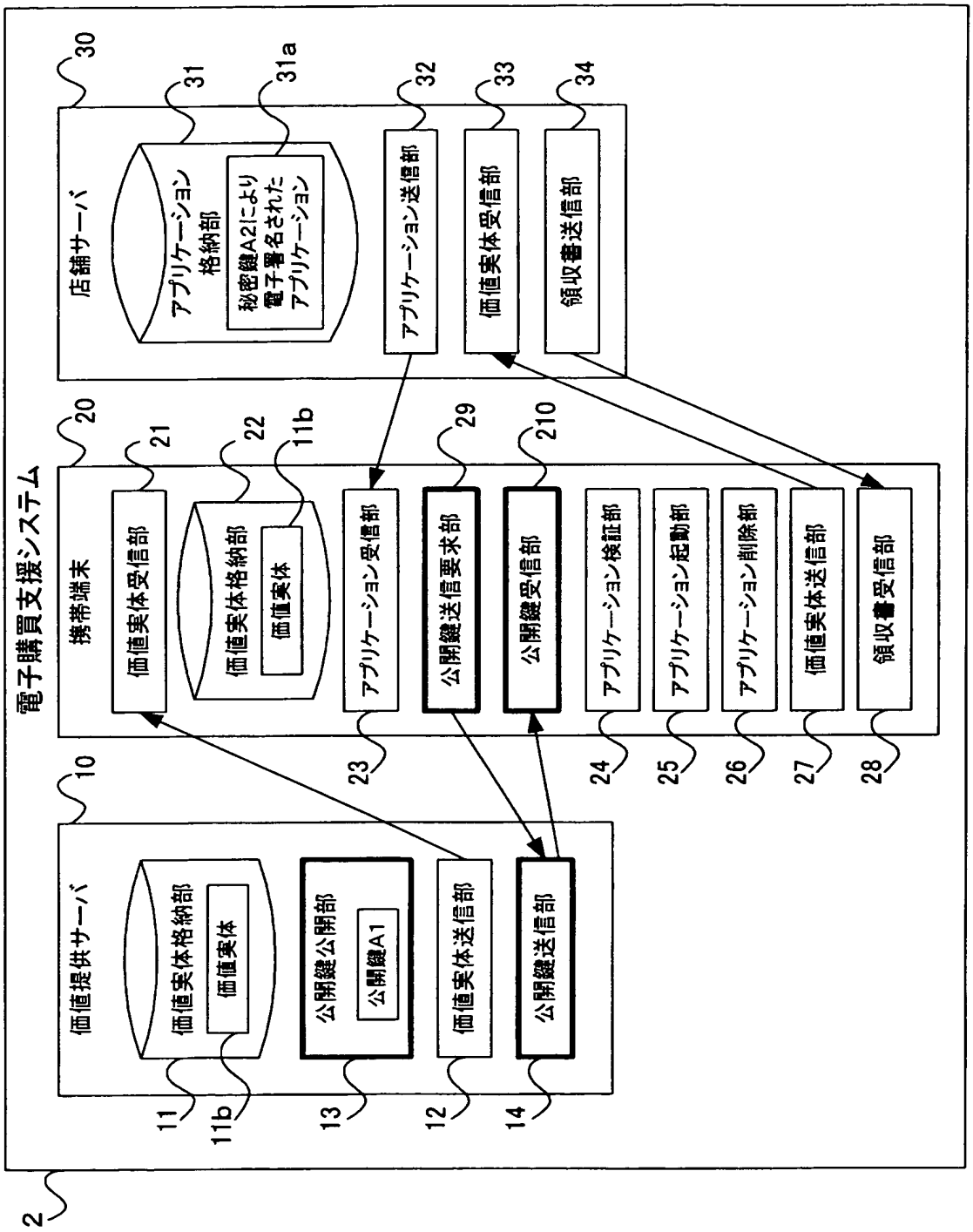
【図６】


表示装置
20d
コーヒーショップメニュー
201
＊＊当店のお薦め＊＊
201a
ドライカフェラテ　350円
＊＊本日のコーヒー＊＊
フレンチロースト　300円
－－メニュー－－
エスプレッソ　300円
カプチーノ　400円
アイスコーヒー　400円

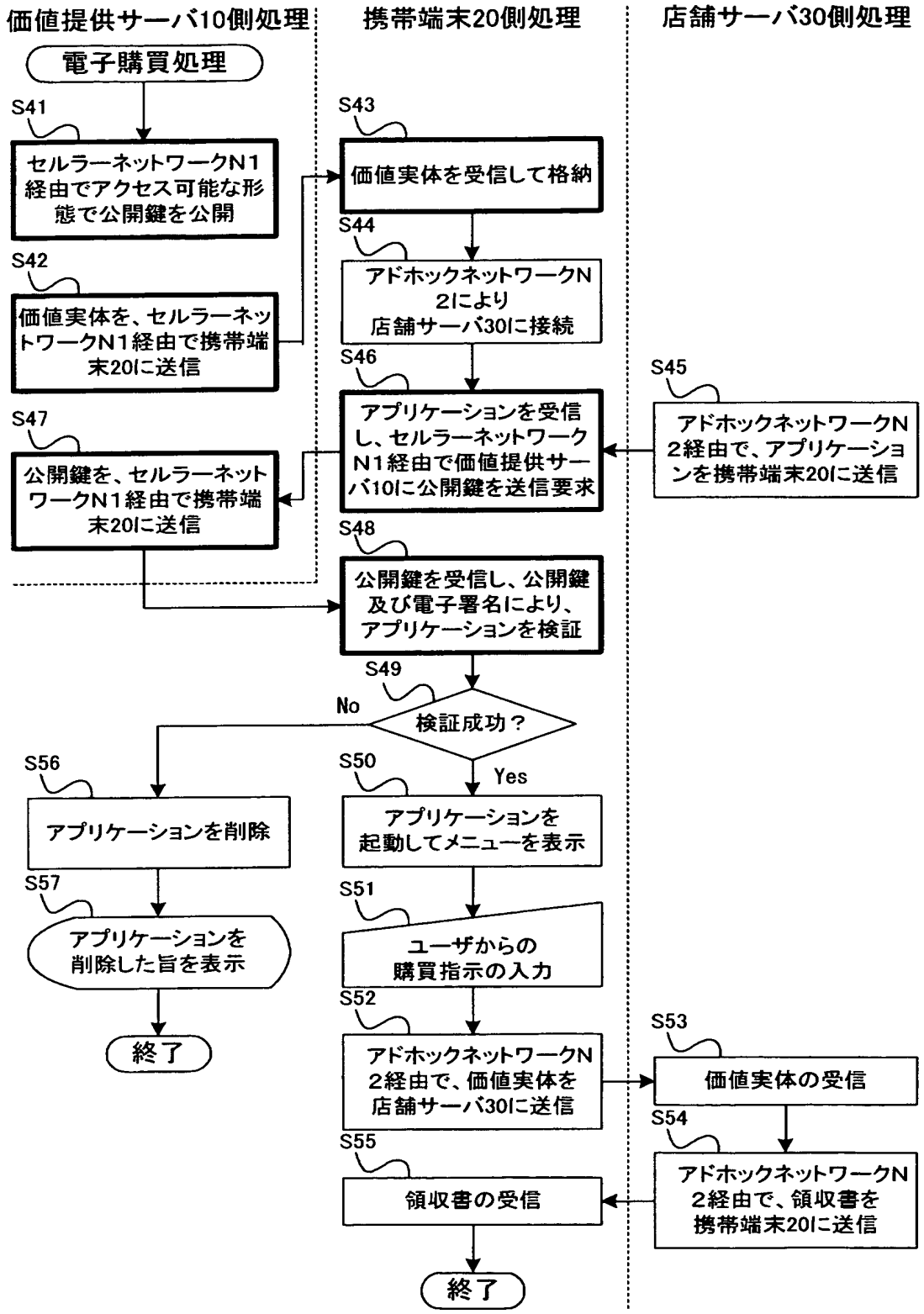
【図７】


価値提供サーバ10側処理
携帯端末20側処理
店舗サーバ30側処理
電子購買処理
S21
公開鍵を、セルラーネットワークN1経由で携帯端末20に送信
S22
公開鍵を受信して格納
S23
価値実体を、セルラーネットワークN1経由で携帯端末20に送信
S24
価値実体を受信し、公開鍵と対応付けて格納
S25
アドホックネットワークN2により店舗サーバ30に接続
S26
アドホックネットワークN2経由で、アプリケーションを携帯端末20に送信
S27
アプリケーションを受信し、公開鍵及び電子署名により検証
S28
検証成功？
No
Yes
S29
アプリケーションを起動してメニューを表示
S30
ユーザからの購買指示の入力
S31
アドホックネットワークN2経由で、価値実体を店舗サーバ30に送信
S32
価値実体の受信
S33
アドホックネットワークN2経由で、領収書を携帯端末20に送信
S34
領収書の受信
終了
S35
アプリケーションを削除
S36
アプリケーションを削除した旨を表示
終了

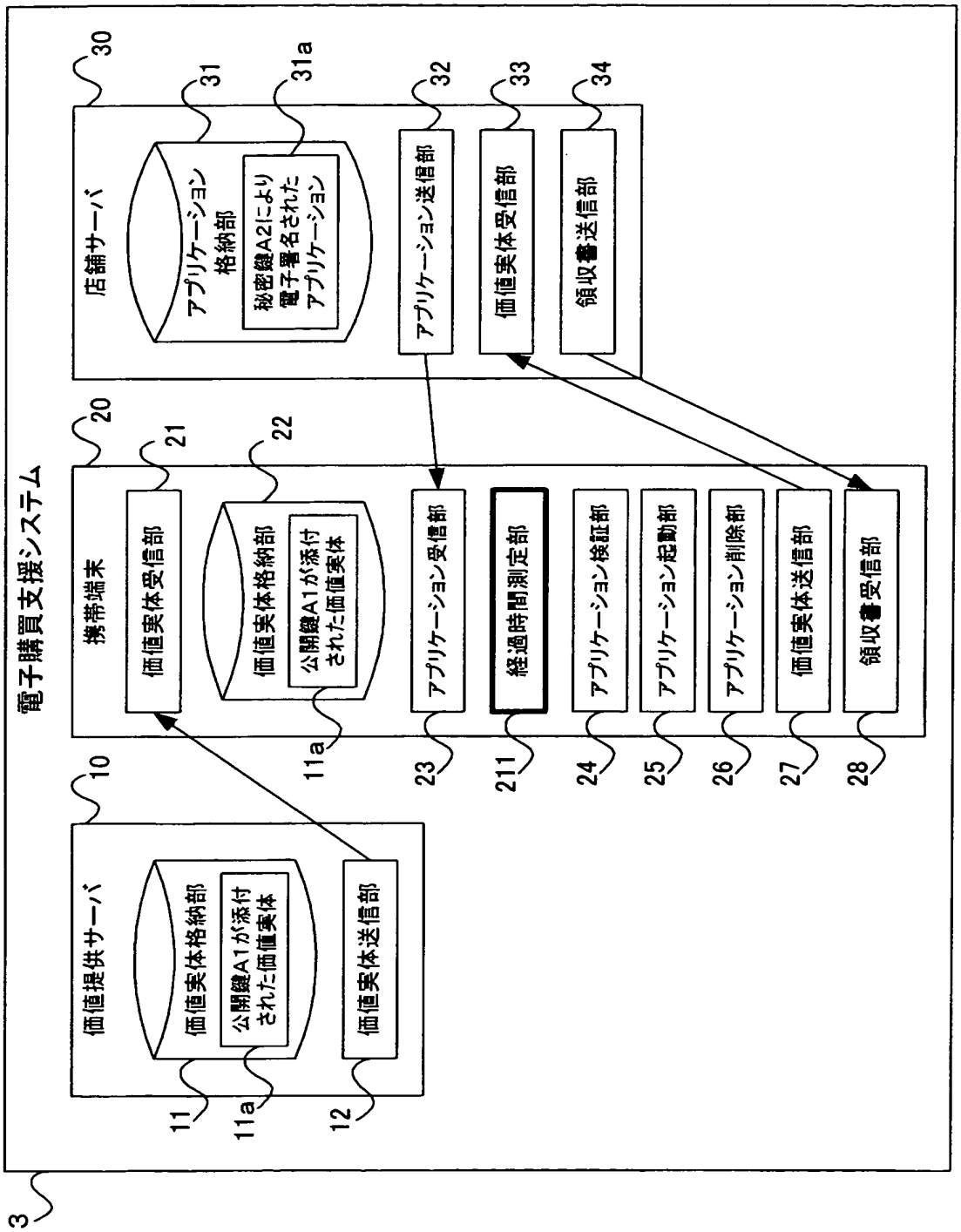
【図８】


電子購買支援システム
2
価値提供サーバ
10
価値実体格納部
価値実体
11
11b
公開鍵公開部
公開鍵A1
13
価値実体送信部
12
公開鍵送信部
14
携帯端末
20
価値実体受信部
21
価値実体格納部
価値実体
22
11b
アプリケーション受信部
23
公開鍵送信要求部
29
公開鍵受信部
210
アプリケーション検証部
24
アプリケーション起動部
25
アプリケーション削除部
26
価値実体送信部
27
領収書受信部
28
店舗サーバ
30
アプリケーション格納部
秘密鍵A2により電子署名されたアプリケーション
31
31a
アプリケーション送信部
32
価値実体受信部
33
領収書送信部
34

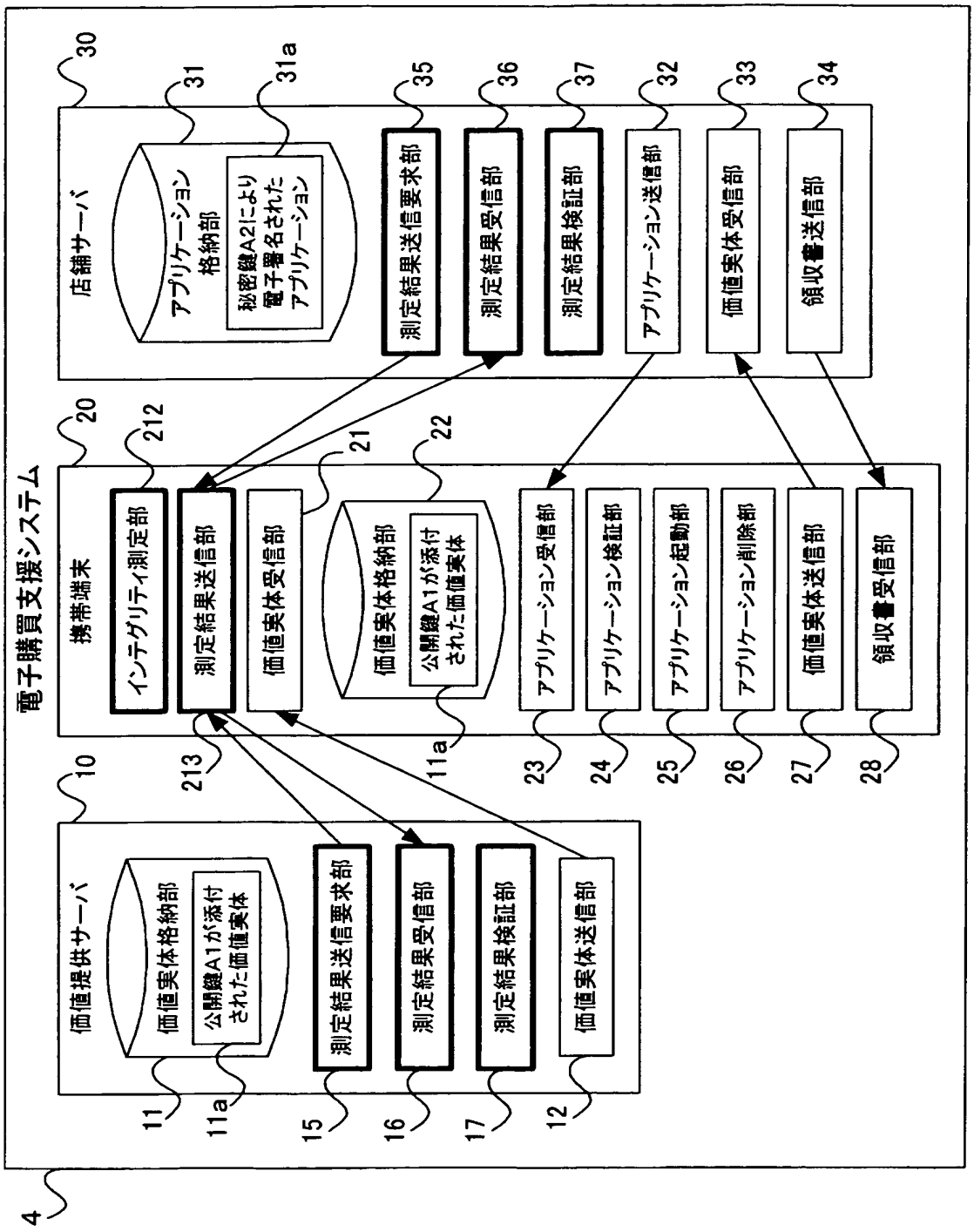
【図９】


価値提供サーバ10側処理
携帯端末20側処理
店舗サーバ30側処理
電子購買処理
S41
セルラーネットワークN1経由でアクセス可能な形態で公開鍵を公開
S42
価値実体を、セルラーネットワークN1経由で携帯端末20に送信
S43
価値実体を受信して格納
S44
アドホックネットワークN2により店舗サーバ30に接続
S45
アドホックネットワークN2経由で、アプリケーションを携帯端末20に送信
S46
アプリケーションを受信し、セルラーネットワークN1経由で価値提供サーバ10に公開鍵を送信要求
S47
公開鍵を、セルラーネットワークN1経由で携帯端末20に送信
S48
公開鍵を受信し、公開鍵及び電子署名により、アプリケーションを検証
S49
検証成功？
No
Yes
S56
アプリケーションを削除
S57
アプリケーションを削除した旨を表示
終了
S50
アプリケーションを起動してメニューを表示
S51
ユーザからの購買指示の入力
S52
アドホックネットワークN2経由で、価値実体を店舗サーバ30に送信
S53
価値実体の受信
S54
アドホックネットワークN2経由で、領収書を携帯端末20に送信
S55
領収書の受信
終了

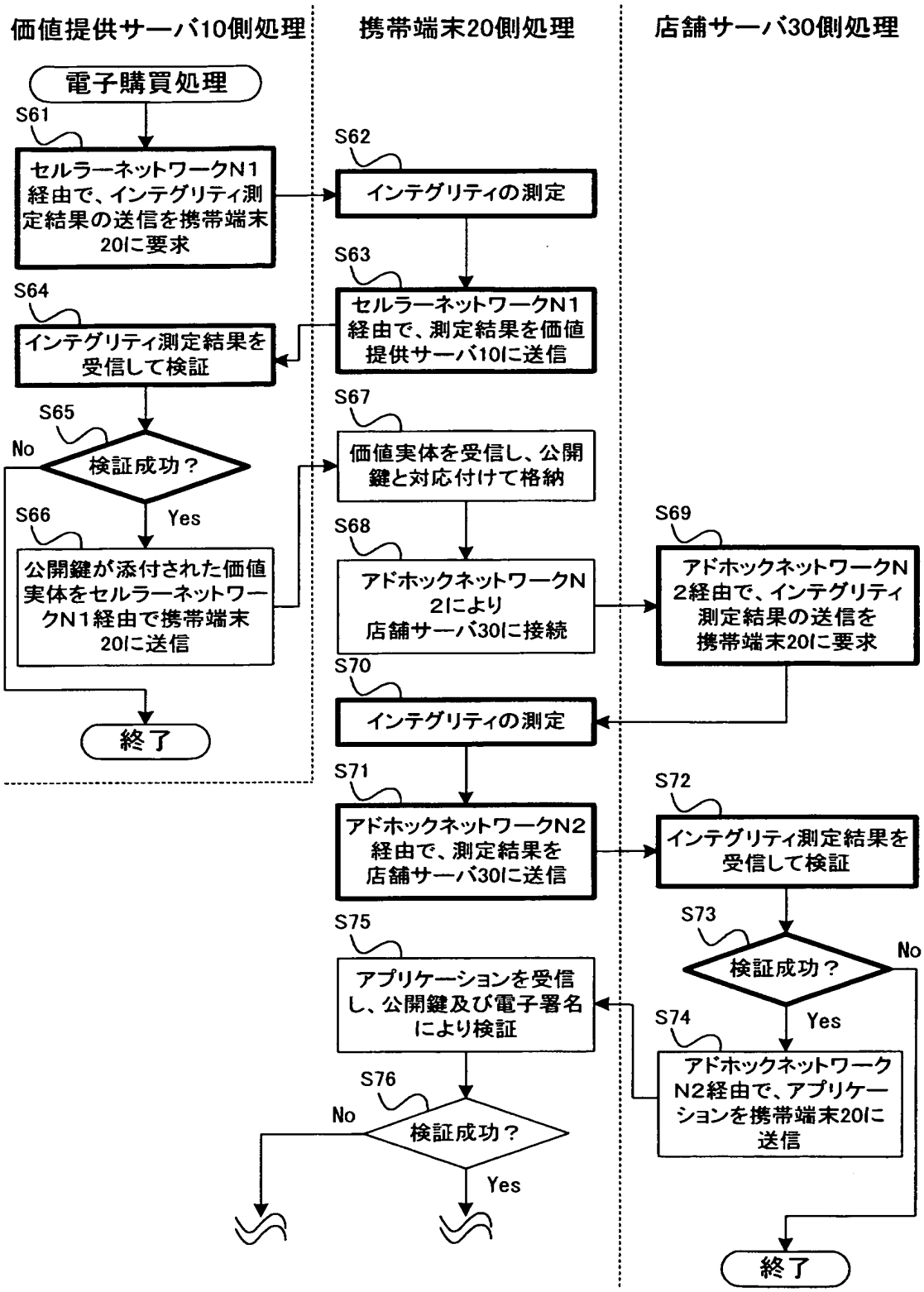
【図１０】


電子購買支援システム
3
価値提供サーバ
10
価値実体格納部
公開鍵A1が添付された価値実体
11
11a
価値実体送信部
12
携帯端末
20
価値実体受信部
21
価値実体格納部
公開鍵A1が添付された価値実体
22
11a
アプリケーション受信部
23
経過時間測定部
211
アプリケーション検証部
24
アプリケーション起動部
25
アプリケーション削除部
26
価値実体送信部
27
領収書受信部
28
店舗サーバ
30
アプリケーション格納部
秘密鍵A2により電子署名されたアプリケーション
31
31a
アプリケーション送信部
32
価値実体受信部
33
領収書送信部
34

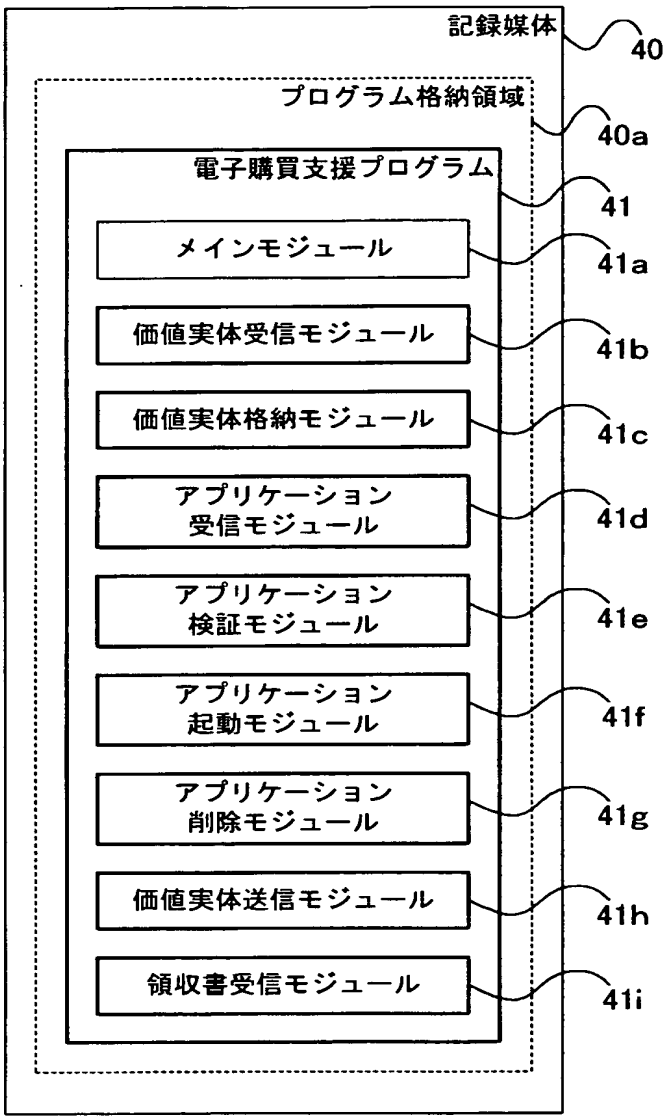
【図１１】


電子購買支援システム
4
価値提供サーバ
10
価値実体格納部
公開鍵A1が添付された価値実体
11
11a
測定結果送信要求部
15
測定結果受信部
16
測定結果検証部
17
価値実体送信部
12
携帯端末
20
インテグリティ測定部
212
213
測定結果送信部
価値実体受信部
21
価値実体格納部
公開鍵A1が添付された価値実体
22
11a
アプリケーション受信部
23
アプリケーション検証部
24
アプリケーション起動部
25
アプリケーション削除部
26
価値実体送信部
27
領収書受信部
28
店舗サーバ
30
アプリケーション格納部
秘密鍵A2により電子署名されたアプリケーション
31
31a
測定結果送信要求部
35
測定結果受信部
36
測定結果検証部
37
アプリケーション送信部
32
価値実体受信部
33
領収書送信部
34

【図１２】


価値提供サーバ10側処理
携帯端末20側処理
店舗サーバ30側処理
電子購買処理
S61
セルラーネットワークN1経由で、インテグリティ測定結果の送信を携帯端末20に要求
S62
インテグリティの測定
S63
セルラーネットワークN1経由で、測定結果を価値提供サーバ10に送信
S64
インテグリティ測定結果を受信して検証
S65
No
検証成功？
Yes
S66
公開鍵が添付された価値実体をセルラーネットワークN1経由で携帯端末20に送信
終了
S67
価値実体を受信し、公開鍵と対応付けて格納
S68
アドホックネットワークN2により店舗サーバ30に接続
S69
アドホックネットワークN2経由で、インテグリティ測定結果の送信を携帯端末20に要求
S70
インテグリティの測定
S71
アドホックネットワークN2経由で、測定結果を店舗サーバ30に送信
S72
インテグリティ測定結果を受信して検証
S73
検証成功？
No
Yes
S74
アドホックネットワークN2経由で、アプリケーションを携帯端末20に送信
S75
アプリケーションを受信し、公開鍵及び電子署名により検証
S76
No
検証成功？
Yes
終了

【図１３】


記録媒体
40
プログラム格納領域
40a
電子購買支援プログラム
41
メインモジュール
41a
価値実体受信モジュール
41b
価値実体格納モジュール
41c
アプリケーション
受信モジュール
41d
アプリケーション
検証モジュール
41e
アプリケーション
起動モジュール
41f
アプリケーション
削除モジュール
41g
価値実体送信モジュール
41h
領収書受信モジュール
41i

【書類名】　要約書

【要約】

【課題】　アドホックネットワークを経由して取得されたアプリケーションを使用して、安全かつ容易に価値実体の授受を行うことである。

【解決手段】　本発明に係る携帯端末２０は、価値実体受信部２１と、アプリケーション受信部２３と、アプリケーション検証部２４と、価値実体送信部２７とを備える。価値実体受信部２１は、秘密鍵Ａ２に対応する公開鍵Ａ１が添付された価値実体１１ａを受信し、受信された価値実体１１ａは価値実体格納部２２に格納される。アプリケーション受信部２３は、秘密鍵Ａ２によって電子署名されたアプリケーション３１ａをアドホックネットワークＮ２経由で受信する。アプリケーション検証部２４は、公開鍵Ａ１を使用してアプリケーション３１ａを検証し、検証が成功した場合には、価値実体送信部２７は、アプリケーション３１ａを使用して価値実体１１ａを店舗サーバ３０宛に送信（移転）する。

【選択図】　図２

特願２００２－３３８５５８

出　願　人　履　歴　情　報

識別番号　　［３９２０２６６９３］

１．変更年月日　　２０００年　５月１９日
［変更理由］　　名称変更
住所変更
住　所　　東京都千代田区永田町二丁目１１番１号
氏　名　　株式会社エヌ・ティ・ティ・ドコモ